REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	2 June 1995	Master's Thesis, 2 Aug 95-7 June 1996

4. TITLE AND SUBTITLE

THE USE OF WORLD WIDE WEB TECHNOLOGY WITHIN THE COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS, AND INTELLIGNECE FOR THE WARRIOR PROGRAM

5. FUNDING NUMBERS

6. AUTHOR(S)

Major JOHN G. LEVINE, U.S. Army

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, Kansas 66027-1352

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/MONITORING

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release, distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

This study investigates the potential for the use of World Wide Web (WWW) technology to support the warfighter. Existing tactical data networks, and command, control, communications, computers, and intelligence for the warrior (C4IFTW) systems are capable of providing WWW services. The Global Command and Control System (GCCS) is capable of using WWW technology to support the deployed warfighter. The C4IFTW program seeks to make C4I services truly transparent to the user by providing a Global Grid with the same level of service available at any location. The same level of service will be available to the warfighter whether in garrison or on deployment. The WWW is a recent development affecting the Internet. The WWW is described as a service that allows users to access text, video, or audio information located throughout the network. The GCCS program is a mid-term solution for the C4IFTW program, it is intended to provide communications capability from the National Command Authority to the Joint Task Force commander. Its capabilities include core planning and assessment functions, as well as the service's readiness support requirements. GCCS is the replacement for the legacy World Wide Military Command and Control System as well as numerous existing stovepipe communications systems.

14. SUBJECT TERMS	15. NUMBER OF PAGES
World Wide Web,C4IFTW,Internet	81
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED

GENERAL INSTRUCTIONS FOR COMPLETING SF 298

The Report Documentation Page (RDP) is used in announcing and cataloging reports. It is important that this information be consistent with the rest of the report, particularly the cover and title page. Instructions for filling in each block of the form follow. It is important to ***stay within the lines*** to meet ***optical scanning requirements***.

Block 1. Agency Use Only *(Leave blank)*.

Block 2. Report Date. Full publication date including day, month, and year, if available (e.g. 1 Jan 88). Must cite at least the year.

Block 3. Type of Report and Dates Covered. State whether report is interim, final, etc. If applicable, enter inclusive report dates (e.g. 10 Jun 87 - 30 Jun 88).

Block 4. Title and Subtitle. A title is taken from the part of the report that provides the most meaningful and complete information. When a report is prepared in more than one volume, repeat the primary title, add volume number, and include subtitle for the specific volume. On classified documents enter the title classification in parentheses.

Block 5. Funding Numbers. To include contract and grant numbers; may include program element number(s), project number(s), task number(s), and work unit number(s). Use the following labels:

C	- Contract	**PR**	- Project
G	- Grant	**TA**	- Task
PE	- Program Element	**WU**	- Work Unit Accession No.

Block 6. Author(s). Name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. If editor or compiler, this should follow the name(s).

Block 7. Performing Organization Name(s) and Address(es). Self-explanatory.

Block 8. Performing Organization Report Number. Enter the unique alphanumeric report number(s) assigned by the organization performing the report.

Block 9. Sponsoring/Monitoring Agency Name(s) and Address(es). Self-explanatory.

Block 10. Sponsoring/Monitoring Agency Report Number. *(If known)*

Block 11. Supplementary Notes. Enter information not included elsewhere such as: Prepared in cooperation with...; Trans. of...; To be published in.... When a report is revised, include a statement whether the new report supersedes or supplements the older report.

Block 12a. Distribution/Availability Statement. Denotes public availability or limitations. Cite any availability to the public. Enter additional limitations or special markings in all capitals (e.g. NOFORN, REL, ITAR).

- **DOD** - See DoDD 5230.24, "Distribution Statements on Technical Documents."
- **DOE** - See authorities.
- **NASA** - See Handbook NHB 2200.2.
- **NTIS** - Leave blank.

Block 12b. Distribution Code.

- **DOD** - Leave blank.
- **DOE** - Enter DOE distribution categories from the Standard Distribution for Unclassified Scientific and Technical Reports.
- **NASA** - Leave blank.
- **NTIS** - Leave blank.

Block 13. Abstract. Include a brief *(Maximum 200 words)* factual summary of the most significant information contained in the report.

Block 14. Subject Terms. Keywords or phrases identifying major subjects in the report.

Block 15. Number of Pages. Enter the total number of pages.

Block 16. Price Code. Enter appropriate price code *(NTIS only)*.

Blocks 17. - 19. Security Classifications. Self-explanatory. Enter U.S. Security Classification in accordance with U.S. Security Regulations (i.e., UNCLASSIFIED). If form contains classified information, stamp classification on the top and bottom of the page.

Block 20. Limitation of Abstract. This block must be completed to assign a limitation to the abstract. Enter either UL (unlimited) or SAR (same as report). An entry in this block is necessary if the abstract is to be limited. If blank, the abstract is assumed to be unlimited.

*U.S.GPO:1993-0-358-779

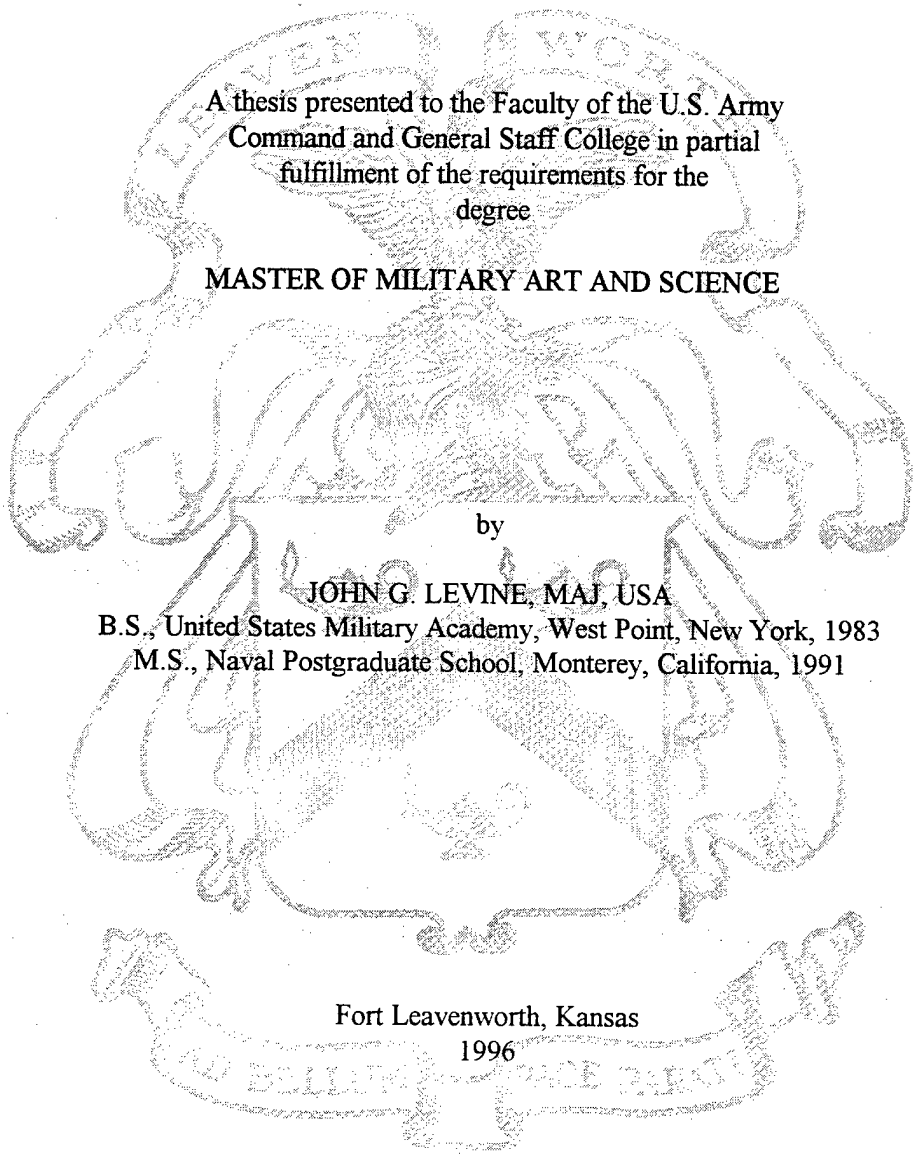
THE USE OF WORLD WIDE WEB TECHNOLOGY WITHIN THE COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS, AND INTELLIGENCE FOR THE WARRIOR PROGRAM

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE

by

JOHN G. LEVINE, MAJ, USA
B.S., United States Military Academy, West Point, New York, 1983
M.S., Naval Postgraduate School, Monterey, California, 1991



Fort Leavenworth, Kansas
1996

Approved for public release, distribution is unlimited.

THE USE OF WORLD WIDE WEB TECHNOLOGY WITHIN THE COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS, AND INTELLIGENCE FOR THE WARRIOR PROGRAM

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE

by

JOHN G. LEVINE, MAJ, USA
B.S., United States Military Academy, West Point, New York, 1983
M.S., Naval Postgraduate School, Monterey, California, 1991

Fort Leavenworth, Kansas
1996

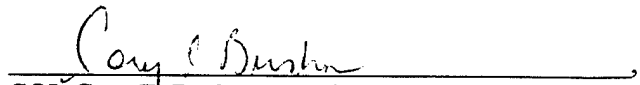
MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

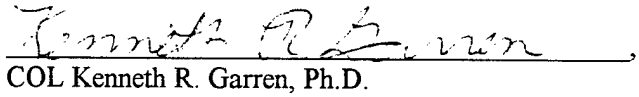
Name of Candidate: MAJ John G. Levine

Thesis Title: The Use of World Wide Web Technology Within the Command, Control, Communications, Computers, and Intelligence Program

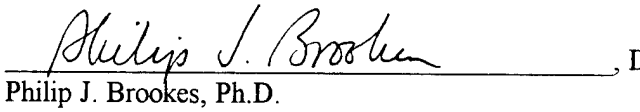
Approved by:


, Thesis Committee Chairman
COL Gary E. Bushover, M.S.


, Member
MAJ Randall L. Mackey, M.S.


, Member, Consulting Faculty
COL Kenneth R. Garren, Ph.D.

Accepted this 7th day of June 1996 by:


, Director, Graduate Degree Programs
Philip J. Brookes, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

THE USE OF WORLD WIDE WEB TECHNOLOGY WITHIN THE COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS, AND INTELLIGENCE FOR THE WARRIOR PROGRAM by MAJ John G. Levine, USA, 71 pages.

This study investigates the potential for the use of World Wide Web (WWW) technology to support the warfighter. Existing tactical data networks, and command, control, communications, computers, and intelligence for the warrior (C4IFTW) systems are capable of providing WWW services. The Global Command and Control System (GCCS) is capable of using WWW technology to support the deployed warfighter.

The C4IFTW program seeks to make C4I services truly transparent to the user by providing a Global Grid with the same level of service available at any location. The same level of service will be available to the warfighter whether in garrison or on deployment.

The WWW is a recent development affecting the Internet. The WWW is described as a service that allows users to access text, video, or audio information located throughout the network.

The GCCS program is a mid-term solution for the C4IFTW program; it is intended to provide communications capability from the National Command Authority to the Joint Task Force commander. Its capabilities include core planning and assessment functions, as well as the service's readiness support requirements. GCCS is the replacement for the legacy World Wide Military Command and Control System as well as numerous existing stovepipe communications systems.

TABLE OF CONTENTS

LIST OF ACRONYMS

ACUS	Army Common User System
AFCEA	Armed Forces Communications-Electronics Association
AFATDS	Advanced Field Artillery Tactical Data System
AGCCS	Army GCCS
ASAS	All Source Analysis System
ATCCS	Army Tactical Command and Control System
ATO	Air Tasking Order
ABCS	Army Battle Command System
ARPA	Advanced research Projects Agency
BBN	Bolt, Beranek, and Newman
BFA	Battlefield Functional Area
BGP	Border Gateway Protocol 4
CE	Collateral Enclave
CHS	Common Hardware/Software
CINC	Commander in Chief
COE	Common Operating Environment
COTS	Commercial-off-the-shelf
COMSEC	Communications Security
CPU	Central Processing Units

CTAPS	Contingency Theater Air Control Automated Planning System
C2	Command and Control
C4I	Command, Control, Communications, Computers, and Intelligence
C4IFTW	Command, Control, Communications, Computers, and Intelligence for the Warrior
DCS	Defense Communications Systems
DCSS	Digital Communications Satellite Subsystem
DDN	Defense Data Network
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DSNET1	Defense Security Network 1
DSNET2	Defense Security Network 2
DSNET3	Defense Security Network 3
DMS	Defense Message System
DOD	Department of Defense
EAC	Echelons Above Corps
ECB	Echelons Corps and Below
EGP	Exterior Gateway Protocol
FTP	File Transfer Protocol
GCCS	Global Command and Control System
GILS	Government Information Locator Service
GMF	Ground Mobile Forces
HTML	Hypertext Markup Language
HTTP	Hypertext Transport Protocol

IGW	Integral Gateway
IP	Internet Protocol
IPR	Internet Protocol Routers
IAB	Internet Advisory board
IETF	Internet Engineering Task Force
ISOC	Internet Society
ITSDN	Integrated Tactical-Strategic Data Network
JFACC	Joint Forces Air Component Commander
JITC	Joint Interoperability Test Center
JOPES	Joint Operations Planning and Execution System
JTF	Joint Task Force
JWICS	Joint Worldwide Intelligence Communications System
JWID	Joint World-Wide Interoperability Demonstration
Kbps	Kilobits-per-second
LAN	Local Area Network
LCU	Lightweight Computer Unit
Mbps	Megabits-per-second
MCS	Maneuver Control Unit
MGV	Mobile Gateway Van
MIB	Management Information Base
MILNET	Military Network
MISSI	Multilevel Information Systems Security Initiative
MLS	Multi-Level Security
MPN	MSE Packet Network

MSE	Mobile Subscriber Equipment
NCTAMS	Naval Computer and Telecommunications Area Master Stations
NES	Network Encryption System
NET ID	Network Identification
NIPRNET	Unclassified-but-Sensitive Internet Protocol Router Network
NRC	National Research Council
NSF	National Science Foundation
NSFNET	National Science Foundation Network
OSPF	Open Shortest Path First
PACOM	US Pacific Command
PC	Personal Computer
PCU	Portable Computer Unit
POP	Point of Presence
PPP	Point-to-Point Protocol
RIP	Routing Information Protocol
SIPRNET	Secret Internet Protocol Router Network
SLIP	Serial Line Internet Protocol
TASDAC	Tactical Secure Data Communications
TCP/IP	Transmission Control Protocol/Internet Protocol
TCU	Transportable Computer Unit
TELNET	Terminal Network Protocol
TNS	Tactical Name Server
TPN	Tactical Packet Network
TRI-TAC	Triservice Tactical Communications

TS-SCI	top secret-special compartmented information
VINES	Virtual Network
WAN	Wide Area Network
WWMCCS	World Wide Military Command and Control System
WWW	World Wide Web

CHAPTER 1

INTRODUCTION

The Problem

Communications technology is an area that has been receiving large amounts of attention in recent times. It is said that the world is entering the "Information Age." The book War and Anti-War by Alvin and Heidi Toffler references three waves in the history of Humanity. These three waves are characterized by the first or Agrarian Wave, the second or Industrial Wave, and the third or Information Wave. Societies that dominate the third wave will be the most prosperous.[1] The coming of the Information Age will have a dramatic effect on many American Institutions, including the US military.

Terms, such as the Internet and the World Wide Web (WWW), are becoming common in today's society. Recognition of the WWW as a universal information database is occurring. Not only is the data on the WWW available to people around the world, but data on the WWW is linked to other data so that information is easily accessible regardless of the data's actual location.[2] The investigation of the WWW as a means of commerce, allowing people to buy and sell products to include information to a global audience, is occurring. Other potential uses of the WWW have yet to be discovered.

The US Military is also devoting attention and resources to information technology. One program is Command, Control, Communications, Computers, and Intelligence for the Warrior (C4IFTW), which seeks to make command, control, communications, computers, and intelligence services truly transparent to the user. The user will have the same level of service at any location, and at this point, the warrior will be operating in the Global Grid. The same suite of command,

control, communications, computers, and intelligence services will be available at all points where the warfighter is deployed.

Programs, such as the Army's Enterprise Strategy, the Navy's Copernicus, and the Air Force's Horizon, are the service component portions of the C4IFTW program. These program are attempting to use information as a combat multiplier on the battlefield. Information allows a commander to get inside an enemy's decision cycle. In these times of declining resources and funding, the military is looking to use information to ensure that the US military maintains its combat edge. The US military also believes that it can use the American edge in technology to its advantage as long as the technology can be rapidly incorporated into the military inventory. "Technology outpaces the Acquisition Cycle."[3] New technology must be rapidly fielded in order for the US military to capitalize on the American edge in technology. Recent advances in computers and communications are areas that have caught the attention of the military. Each service component of the C4IFTW program attempts to rapidly employ advances in these areas.

Individual services developed current tactical communications systems to meet their individual requirements. These systems are "stovepipe" systems in that they only address the needs of one component. Stovepipe communications systems are vertical as opposed to horizontal in orientation. Currently, information needs to be passed from one component to another component, traverse all the way up one component's stovepipe system, possibly all the way back to the sustaining base in the Continental United States (CONUS), then traverse down the other service's stovepipe system, and ultimately reach the final destination. This hierarchy wastes precious bandwidth resources and severely restricts operational flexibility of the deployed forces.

The US Military is seeking to provide a Global Grid for the warrior. The Global Grid will address future command, control, communications, computers, and intelligence services.

> Global Grid is a concept for end-to-end protected seamless multi-gigabit information transfer and processing capability whenever and wherever it is needed, transparent across ground, air, space, and sea systems, using international open systems and standards and commercial off the shelf technology.[4]

Global Grid is a concept, not a network. The network that will implement the strategic portion of Global Grid is the Defense Information Systems Network (DISN) provided by the Defense Information Systems Agency (DISA). Global Grid provides a real-time representation of the battlespace from a communications aspect.

The battlespace is defined as an area over which the warfighter exercises military control. For communications the battlespace could possibly be worldwide. The Global Grid would provide soldiers, airmen, sailors, or marines with the same suite of services no matter where they are deployed. There would be no difference in information requests or transfers made from a ship or from the battlefield to a location in the sustaining base. The Global Grid would blur the lines between the strategic and tactical networks, if not eliminate the differences completely.

At present the warfighter uses two sets of communications systems, one system is used when in garrison and another system is used when deployed. The use of two separate systems results in personnel requiring training in the use of two separate types of communications systems. The need for this training is a waste of resources and a duplication of effort to accomplish the same function.

Many of the services that the WWW will provide are services that the military may be interested in using on the battlefield. Requirements such as "smart push-warrior pull" can be addressed by capabilities available from the WWW. Smart push-warrior pull is the capability for warfighters to access a communications network and have the necessary, timely, and relevant information pulled (initiated by a warfighter request) or pushed (based on a previously developed warfighter profile) to them.[5] The smart push-warrior pull capability should be available anywhere on the battlefield. At the present time, there is not a military network in place to provide this type of service. This capability is very similar to the services that are provided on the Internet and the WWW.

The US military does not have the resources necessary to develop a totally separate and militarized WWW capability. Separate networks, however, have been developed by the military to

address the various information classification levels. In the future, all information, no matter what the classification, will traverse the same network. The systems that the military is developing to meet the information requirements of the warfighter must be capable of providing WWW types services, such as the ability of a user on one computer to access information stored on another through a communications network regardless of the operating system running on the computers.[6] It must be a system which the warfighter is comfortable and familiar with. The system must stay current with emerging technology. Most of all, this communications network must provide the services that the warfighter needs anywhere that the warfighter is deployed. Software, protocols, and procedures developed by the commercial sector could be used by the military in the development of the Global Grid. The military must look to the commercial sector to determine what technology is available to meet the requirement of C4IFTW. Commercial products could possibly provide the necessary services at the most economical price.

Research Question

This thesis will examine some of the recent developments in civilian and military communications to include C4IFTW, the Internet and the WWW. The research question is stated as follows: How can the C4IFTW program use the WWW? This thesis will examine the various capabilities of the current and future C4IFTW program at both the strategic and tactical levels. It will also examine the capabilities and requirements of the Internet and the WWW. Both must be examined to determine how their capabilities can be incorporated into the C4IFTW program.

The first supporting research question that this thesis will address asks the following: Does the military possess the equipment and communications necessary to provide the WWW for the C4IFTW program? The type of equipment used determines the level of service that is provided to the user. More complex equipment may provide a greater level of service.

A subsequent research question asks the following: How can the WWW support the warfighter within the C4IFTW program? An examination of WWW technology will show how this technology functions and how it can be used to support the warfighter.

Assumptions

An Internet type of network with WWW capability must be available in order to implement the WWW for the C4IFTW program. This thesis will assume that at the unclassified security level, access to both the Internet and the WWW will be available on the battlefield. The U.S. military, under the C4IFTW program, is attempting to move away from stovepipe communications to a common user type of communications system. The best examples of common user communications networks are the Internet and the WWW services that it provides.

This thesis will also assume the current data or packet switching capabilities of the services will be all that is available on the battlefield in the near term. The services do possess packet switching capabilities. Packet switching is similar to using the mail to complete the transfer of information from one location to another. If a message was broken up into standard size parts (packets) and sent through the mail, they would eventually arrive at the destination. There is no guarantee that each packet would follow the same route, and it would be up to the destination to reconstitute the original message from the parts it received. All of the services presently possess limited capabilities for packet switching and these capabilities may be upgraded sometime in the future. This thesis will examine the present capabilities to determine if the WWW can be implemented on the battlefield in support of the C4IFTW program.

Limitations

At present, there is little information available on the capabilities of strategic information systems to incorporate the WWW. Many of these systems are in the process of transitioning from stovepipe systems to common-user systems. The new architecture of these automated information systems may not yet be finalized. The availability of data from these program offices was a limiting factor in completing this thesis.

Delimitation

Both the Internet and the WWW offer limited security of data at the present time. The U.S. military is investigating the use of multi-level security (MLS) products that will allow for higher security information to traverse a network with a lower classification level. These products work by encrypting information at both ends of the network that the information is traversing. True MLS, which allows for workstations at one security level to talk to workstations at another security level on the same network, does not yet exist. At present limited MLS capabilities exist that allow information at one security level to traverse a network at a different security level as long as this information is encrypted before traversing the other network. MLS within the C4IFTW program will allow for the conservation of bandwidth and the consolidation of information on tactical networks. This thesis will not examine true MLS capabilities but will examine limited security capabilities that currently exist that provide for single level security.

Another area being investigated is that of bandwidth efficiency. There is never enough bandwidth on the battlefield to provide all the information that the commander requires. Work is ongoing in areas of data compression and bandwidth on demand types of communications to allow for the transfer of audio and video information. This thesis will not examine bandwidth on demand capabilities but will examine emerging technologies in the area of data compression that may allow for the transfer of audio and video information.

Data Networks

The Internet and the World Wide Web (WWW)

The Internet is many different things to many different people. The most common term describing the Internet today is the "Information Superhighway." Some of the definitions that describe the Internet are a collection of networks, a sharing of resources that can be reached from various networks, or a community of individuals who use and develop the networks. The Internet can also be thought of in relation to its protocols, where protocols are described as a mutually

agreed upon method of communications between two parties. In addition to these common protocols, the Internet also has gateways to allow connections to other networks utilizing other services and protocols.[7] The Internet can be thought of as a Global Grid of various computer networks.

The Internet was established 25 years ago by the US Department of Defense to support military research. The agency tasked with developing this network was the Advanced Research Project Agency (ARPA). The ARPA was attempting to build a network that could withstand a nuclear attack and still provide communications. Communications in the ARPA model occurs between source and destination, and the network itself was considered to be unreliable, i.e., portions of the network could disappear at any time. Packet switching ensures that communications were accomplished. All computers on the Internet are considered peers and are able to communicate with all other computers on the network.[8] The Internet has evolved past the use that was initially envisioned for it by ARPA.

Other scientific communities besides ARPA began to build their own computer networks during this time span to include the National Science Foundation (NSF), who created the National Science Foundation network (NSFNET). The NSFNET was initially established to connect five NSF supercomputing centers to allow expensive supercomputing resources to be available for scholarly research. Since only five centers were created, a way needed to be developed to allow users to access them. The NSF developed a network, based on the ARPA network, which allowed for easy connection between the two networks. The sharing of supercomputer centers allowed connected users to access other resources not associated with the centers. The ability of connected users to access data and individuals resulted in a growth in the popularity of the Internet.[9] Other organizations began to develop their own networks that could be connected to the growing Internet.

The Internet is not managed by any one agency or corporation, but the ultimate authority for Internet policy rests with the voluntary Internet Society (ISOC). ISOC's purpose is the promotion of global information exchange. Standards for the Internet are established by the

Internet Architecture Board (IAB) and the Internet Engineering Task Force (IETF). These organizations develop standards that allow computers from different vendors to communicate with each other.[10]

The Internet is not one vast global network, but a collection of many different networks that are able to communicate with each other. The C4IFTW effort is attempting to develop a program that will connect the many different tactical and strategic Department of Defense (DOD) communications networks. There are many similarities between the Internet and the C4IFTW program.

The WWW is a recent development affecting the Internet. the WWW is described as a service that allows users on the network to access information located anywhere on the network. This information can be in the form of text, video, or audio and the amounts of information available on the Internet is enormous.

Hypertext capabilities allow for the linking of information for the WWW. Hypertext documents are accessed through a home page at one location. Home pages are a collection of information that is maintained by an organization. Hypertext documents, accessed on one home page can be hyperlinked to hypertext documents accessible through another home page at a different location.[11] This is the beauty of the WWW. Users can start at one location and collect information from a variety of sources at other locations without having to manually change locations each time they request information from another source.

Department of Defense Strategic And Tactical Data Information Systems

At present two major communications networks exist within the DOD. The first network is the strategic network. This network is installed, operated, and maintained by DISA, who is responsible for all of the communications between posts, camps, and stations belonging to the DOD. This network is known as DISN, and its current data networks consist of four separate subnetworks. There are separate network at each security level.[12] These networks offer the best opportunity to provide the WWW at the strategic level.

MILNET was the network that is established at the unclassified level. MILNET was a packet-switched based network utilizing 64 kilobits-per-second communications paths between switches. It was replaced in October 1995 by NIPRNET. NIPRNET stands for Sensitive-But-unclassified Internet Protocol (IP) Router Network. It is a router-based network that uses communications paths between 56 kilobits-per-second and T-1 rates (1.544 megabits-per-second). Router-based networks offer more flexibility than packet-switched based networks by allowing for dynamic redirection of network traffic in the event of failure within the network. Increased communications paths between routers provide increased capabilities to transmit data on the network.

DSNET1 was the secret-level network. It was also a packet-switched network having the same capability as MILNET, except that it was statically routed. Static routing is routing that follows a fixed predetermined path from one location to another. It is very labor intensive to maintain and reconfigure. DSNET1 was replaced by SIPRNET in October 1995. SIPRNET stands for secret Internet Protocol (IP) Router Network. It is also a router-based network that uses communications paths between 56 kilobits-per-second and T-1 rates (1.544 megabits-per-second). It will dynamically route information throughout the network.

DSNET2 is the current top secret network whose primary user is the World Wide Military Command and Control System (WWMCCS). WWMCCS is scheduled for replacement sometime in the near future with the Global Command and Control System (GCCS). Each service is building its own portion of GCCS that will fit into the joint program. GCCS will operate at the secret level and can therefore traverse SIPRNET. Once the transition from WWMCCS to GCCS occurs, DISNET2 will be dismantled. There is no replacement network planned for DSNET 2.

DSNET3 was the top secret special compartmented information (TS-SCI) Network. DSNET 3 was replaced by the Joint Worldwide Intelligence Communications System (JWICS). This network provides both data and video teleconferencing services by combining separate types of data over the same circuit.

One of the goals of the C4IFTW program is elimination of the separate communications networks for each security level.[13] Before this transition occurs, there will be three remaining separate networks: NIPRNET, SIPRNET, and JWICS. Ultimately, this information will traverse the same network.

DISA has already begun implementation of a program which enables DOD to transition to the Global Grid architecture. This program, directed by the Joint Staff, is known as the Integrated Tactical-Strategic Data Network (ITSDN) program. Its origin is based on the noted deficiencies in the ability to establish data communications among the services and from the services to the strategic networks. The primary deficiency noted was the tactical community's inability to communicate to the sustaining base. An additional shortfall identified was the lack of data connectivity between the deployed services. The Joint Staff recognized this shortfall and directed the establishment of the ITSDN program.[14]

The ITSDN program was established as a three-phased program. The goal of the first phase is to establish initial connectivity between the services and from the services to the strategic network. This phase is still characterized by gateways and black box/special cable types of devices and is very manpower intensive when it comes to establishing and maintaining these data networks. Separate networks are still maintained for each security level in this phase. This is the phase that will be addressed within this thesis. Once connectivity is established and documented, the ITSDN program can move on to phase two.[15]

The second phase of the ITSDN program is the identification and implementation of security products within the ITSDN networks at both the tactical and strategic level. This phase of the program is directly related to the security product work that is being accomplished under the Defense Message System (DMS) being developed by DISA and the Multilevel Information Systems Security Initiative program (MISSI) by the National Security Agency.[16] These programs will combine information of different security levels over a single network. This capability is not available at present and will not be addressed within this thesis. The use of a single network by the

military will have a significant impact on the tactical community; because once there is no longer a need for separate networks for each security level, the requirement to establish duplicate networks is eliminated. A single network will result in a savings of equipment and personnel. With the current doctrine of a force projection military, the requirement for a single network will reduce the lift requirement for communications equipment and personnel without reducing communications capability. This phase will still be characterized by gateway, black box solutions, and manpower intensive networks.

The third and final phase of the ITSDN program is the objective phase. The goal of this phase is a single seamless network carrying all levels of security. The network itself will be truly "colorless," i.e., an unclassified network, while the information on the network will be at various classification levels.[17] When this is accomplished, networks will no longer be classified, only the information on the networks will be classified as necessary.

The final phase of the ITSDN network will have a major impact on the C4IFTW program. Although the ITSDN program is initially intended to provide data services (electronic mail (e-mail), FTP (file transfer protocol), and TELNET (remote log-on capability)), it will ultimately carry the bulk if not all of the voice, message, and video services in addition to data. The current ITSDN solutions are based on the physical separation between the two networks--SIPRNET and NIPRNET.

DISA has established a program which allows for tactical-to-strategic data connectivity. This program, known as the Point of Presence (POP), establishes tactical to strategic connectivity as part of the ITSDN program. A suite of POP equipment will be installed at ten tactical-to-strategic gateway locations.[18] The equipment installed at the POP locations will be critical for the tactical use of WWW services on the strategic network.

The DISN ITSDN POP gateways will consist of commercial Wellfleet Link Node Routers located at Digital Communications Satellite Subsystem (DCSS) Ground Mobile Forces (GMF)

Entry Points.[19] These gateway routers will be used to support Joint Task Force (JTF) contingencies that have requirements to operate with Internet Protocol Routers.

The ITSDN POP gateways will consist of an unclassified router, a secret router, cryptographic equipment, and other ancillary devices. Two routers will be installed at each of the ten different strategic entry points. [20] The twenty routers are divided into two sets of 10 routers each based on the classification of data they process. Ten routers will connect JTFs to the strategic network at the secret level wide-area backbone router system (SIPRNET). It is a replacement for the current X.25 based DSNET1 network. The other ten routers will connect JTFs to the strategic network on the unclassified level wide-on backbone router (NIPRNET). It is a replacement for the current X.25 based MILNET network.[21] The twenty POP Wellfleet routers were installed by the end of the first quarter, fiscal year 1995.

The location of the ITSDN POP Wellfleet routers is addressed in the DISN ITSDN Internet Protocol Addressing Plan, dated 24 June 1994. The connectivity of the Wellfleet POP routers to the various tactical data networks was validated during the Joint Interoperability Test Center (JITC) Major Switch Test held during third quarter, fiscal year 1995.

A brief description of the type and location of the packet switching equipment follows to provide information on the extent and capability of the tactical packet network. This information will provide possible locations for the WWW within the deployed network.

Army Systems

The Army Tactical Packet Network (TPN)

The TPN is a secret-high system and can only process information up to that level.[22] Until a true MLS system is developed, the TPN will remain secret-high. The only type of WWW services that can be accessed by the current TPN are those at the secret level.

The TPN includes the packet switching overlays fielded at Echelons Corps and Below (ECB) and Echelons Above Corps (EAC). The Army Mobile Subscriber Equipment (MSE) overlay at ECB, referred to as the MSE Packet Network (MPN), began fielding in September 1991

and is now complete. The Triservices Tactical Area Communications (TRI-TAC) packet overlay, at EAC, is on contract and is in the middle of fielding.

The packet switch used in the TPN is a variation of the Bolt, Beranek, and Newman (BBN) C3 packet switch and is a self-contained unit called the C/3-XA or the AN/TYC-20. The purpose of the switches is to provide user access and to route packets through the MSE network.[23] To accomplish this, the C/3-XA contains two separate processors. One of the processors used is the main processor which handles all the packet-switching functions. This processor automatically switches and routes data in the form of packets. The other processor is the integral gateway (IGW) which acts as a transparent gateway to all local area network (LAN) hosts.

Another switching component of the TPN is the AN/TYC-19 (T/20) router. Its purpose is to interconnect three different IP networks.[24] These different networks may be networks with different network identifications (NET IDs) or other types of local and wide area networks (Defense Data Network (DDN), TASDAC, etc.). The AN/TYC-19 provides up to three port interfaces, hence the interconnection of three different networks.

Users may gain access to the TPN through LAN connections, direct host connections, or through dial-up connection over telephone circuits. Commercial-off-the-shelf (COTS) hardware and software have been tested and are being used on the TPN. LAN connections are limited to 185 meters from the MSE shelter while direct host and dial-up connections can be established from greater distances.

The TPN is a commercial, standard-based network. Some modifications were made better to support tactical users in a highly mobile environment. For example, the direct host connection mentioned in the above paragraph better supports tactical users, especially since users cannot always position themselves in close proximity to the packet switch due to terrain and mission constraints. Its tactical name server (TNS) supports tactical users by providing for high mobility. In a static environment, users are assigned permanent Internet Protocol (IP) or numerical addresses. Those addresses can be entered into host tables and configuration files by skilled

system administrators, and the addresses do not often change. In the tactical environment, users and their computers move on a regular basis, and equipment can be damaged or destroyed. The automatic registration capabilities of the TNS allows users to retain the same plain language name for their computers, while their IP addresses change because of high battlefield mobility and network changes. The TPN users do not need highly skilled system administrators to help them connect to the TPN, because automatic address acquisition and registration software can do the system-administrator tasks for them.

The TPN was fielded to support the Army battlefield functional areas (BFAs). The BFAs are all components of the Army Battle Command System (ABCS). The goal of the ABCS program is to build a battle command system that is flexible, interoperable, tailorable, and responsive to the battle commander. ABCS is an umbrella concept that encompasses command and control systems (C2) and the Army Tactical Command and Control System (ATCCS) at all echelons and seeks to integrate all C2 systems to include the BFAs. The components of ABCS include all computers available under the Common Hardware/Software (CHS) 1 and 2 contracts. Components of the CHS 1 and 2 contracts include transportable computer units, lightweight computer units, and handheld computer units along with common software. The BFAs will use computers from the CHS 1 and 2 contracts, and these computer systems are currently arriving in the tactical arena.[25] These BFAs include the Army Tactical Command and Control Systems (ATCCS), Advanced Field Artillery Tactical Data Systems (AFATDs), All Source Analysis System (ASAS) Collateral Enclave (CE) (Intel Fusion), Combat Service Support Control Systems (CSSCS), Forward Area Air Defense (FAAD) Force Operations (FO), and the Maneuver Control System (MCS) PHOENIX. Many of these systems are not yet packet network compatible, but this capability will exist with the use of the CHS 1 and 2 computer systems.

The efficiencies of the TPN are also its limitations. The TPN is overlaid onto the voice network and, as a result, only a small amount of bandwidth is available for data. It is projected that the TPN will be flooded with data once the BFAs begin to connect to it. It is also difficult to

connect the TPN to other router-based networks with communications paths larger than a 16 kilobits-per-second dial-up port. Communications security (COMSEC) equipment (KG-94) to provide bulk (encrypting multiple channels) encryption and two Line Termination Units (black boxes) are required if data rates greater that 16 kilobits-per-second are desired to connect the TPN to another router-based network. The TPN may be able to be modified to use link encryption to encrypting a single channel. A demonstration of both techniques occurred during the Joint Worldwide Interoperability Demonstration (JWID) in 1994; however, both of these solutions are very manpower and engineering intensive.

Mobile Gateway Van (MGV)

The MGV is intended to provide unclassified but sensitive connectivity for deployed Army units. It will extend MILNET/NIPRNET to the battlefield and provide e-mail host capability.[26] It will allow tactical users direct connection or dial-up access to the MGV where unclassified traffic can be sent to/from the area of operations to CONUS or other military activities worldwide. It is a forward-deployed MILNET/NIPRNET host and will provide all MILNET/NIPRNET service to tactical users.

The Army is using other alternatives to allow for tactical connectivity to NIPRNET on the battlefield. These alternatives include the use of security devices, such as the Motorola Network Encryption System (NES) to encrypt unclassified packet data so it can traverse the secret TPN to get to NIPRNET at the strategic level.

There are numerous Army computer systems that will require ITSDN access. There are over 350 computer systems that support Combat/Combat Support/Combat Service Support functions. A vast majority of these systems will require ITSDN access for the transfer of information. At present, many of these systems are either stovepipe or stand-alone, i.e., not communicating with any other system.

The Army is at present a power projection force. The concept of split-based logistics, a component of power projection, relies on assured communications systems that allow much of the

logistical base to remain in CONUS, receive and act on information, and send necessary supplies forward. This concept will depend heavily on ITSDN and WWW capabilities. As long as the automated data systems required for the forward-deployed Army elements are able to connect to the TPN or MGV , ITSDN and the WWW will be able to work for a split-based scenario, provided the necessary common communications assets are available at the tactical level.

Air Force Data Systems

Tactical Secure Data Communications (TASDAC)

TASDAC was developed to provide a deployable and secure data communications capability that interfaces with existing Air Force tactical communications equipment/networks. It is intended to provide interfaces to and compatibility with the fixed data networks to include MILNET/NIPRNET and DSNET1/SIPRNET. It is available in both a deployed-node and fixed-node configuration. The fixed node allows the Air Force to maintain a "reach back" (tactical-strategic gateway, similar to the ITSDN POP) for its deployed units. Deployed TASDAC consists of a user interface and a network interface. TASDAC uses a Wellfleet link node router. The user interface consists of: LAN interfaces, wire interfaces, and dial-up interfaces.

TASDAC is not overlaid onto the Air Force Circuit Switched Network and requires the use of interface devices to interconnect TASDAC nodes that are not hard wired together. What the Air Force gives up in efficiency it gains in compatibility. Since TASDAC circuits can be link encrypted using KG-84As, they can connect to other commercial routers and to POP routers in an easier manner than the Army TPN.

At present, two TASDAC nodes are used on a deployment, one for secret traffic and one for sensitive but unclassified traffic. In the future when an MLS system is available, one TASDAC node will be used for both levels of traffic. The Air Force is currently investigating the Motorola NES to allow for this capability. The Joint Communications Support Element uses TASDAC to support deployed JTFs.

Air Force programs that use TASDAC include the Contingency Tactical Automated Planning System (CTAPS), which is the system used by the Air Force to develop the Air Tasking Order (ATO). In a joint environment, the Joint Forces Air Component Commander (JFACC) uses CTAPS to develop the ATO for the entire theater. Manual means were used in the past to distribute this information on air tasking orders to the various components of the JTF. The CTAPS program is one that has the potential to use WWW technology for distribution of the ATO automatically through the communications network to the JTF. CTAPS is a component of the GCCS program and will be examined in chapters three and four of this thesis.

Both the Army TPN and the Air Force TASDAC use the Exterior Gateway Protocol (EGP) as an exterior routing protocol. Exterior routing protocols provide the means through which information is exchanged with exterior neighbors outside the TPN or TASDAC autonomous system. EGP is an existing protocol that has been in use for a number of years. Both the Army and Air Force are upgrading to the Border Gateway Protocol (BGP). EGP is less efficient and less flexible than BGP. EGP cannot detect routing loops, while BGP can.

The DISN data network is also converting to BGP, to include the Wellfleet routers used at ITSDN POP gateways. BGP has an enhanced capability to support localized router-based host groups. It requires more memory and computational power but requires considerably less bandwidth, resulting in a good tradeoff since bandwidth is a precious resource on the modern battlefield.

This upgrade to BGP will greatly simplify tactical-to-tactical and tactical-to-strategic connectivity between the services. It enables the services to reach WWW servers that are located in both adjacent services, the strategic networks, and on the Internet.

Marine Corps Systems

The Marine Corps currently use the Banyan Virtual Network (VINES) for its Local Area Networks (LANs).[27] Banyan VINES implements a distributed network system based on a proprietary protocol derived from the Xerox Network System (XNS). A distributed system

environment permits transparent exchange of information between clients (host computers) and servers (specially designated computers that provide services, such as file and print service). the WWW is based on this same principle of a distributed system environment.

The Marine Corps uses specialized commercial hardware to connect to the DISN and other military services. Special interface devices are required to connect the Marine Corps and the Army TPN.

Navy Systems

The Navy uses packet-switched systems to interconnect tactical elements (afloat) with the shore. Both afloat and onshore capabilities include IP routers which supplement access to strategic systems. At present, deployed Naval forces are unable to connect directly with other services. These forces must first connect with their Naval Computer and Telecommunications Area Master Stations (NCTAMS) in order to access DISN and the other services.[28]

Global Command and Control System (GCCS)

The GCCS program was developed to meet the needs of the warfighter on the joint level and is intended to provide the implementation for the C4IFTW concept on the battlefield. It is intended to be a midterm solution for the C4IFTW program that will provide a capability for communications from the National Command Authority to the JTF commander and will use commercial hardware and software that will provide the capability for smart push-warrior pull on the battlefield both horizontally and vertically across command levels.[29] GCCS will consist of joint and individual service unique components and its capabilities will include core planning and assessment functions required by the CINCs and JTF commanders, as well as the readiness support requirements of the individual services. It will also incorporate unique regional and functional information requirements.[30] GCCS is the intended replacement for the stovepipe WWMCCS system as well as numerous existing command unique systems to include the EUCOM

Strategic Tactical Army Command and Control System and the PACOM Theater Command and Control System.

GCCS is based on a client server model that will provide current operational data to the CINCs as well as a graphical representation of the tactical picture of the battlespace.[31] The requirements to provide current operational data and graphical information of the tactical situation are application lends themselves to WWW technology. This thesis will examine the capability for GCCS to host the WWW. Components of GCCS will be reviewed and analyzed in Chapters Four and Five.

Significance of the Thesis

The Department of Defense continues to examine the area of communications in order to improve the capabilities provided to the warfighter. The individual services also continue the examination of their individual communications capabilities in order to find ways to provide more communications capabilities with fewer resources. All of the services are attempting to use information to offset their reduction in manpower and to use technology in order to dominate the information spectrum on the battlefield.

The communication systems described in this chapter provide current DOD tactical and strategic data communications capabilities. These are the systems that must be examined to determine where the WWW can be provided to the warfighter. The WWW will most likely provide the warfighter with increased capabilities at a lower cost than present data distribution systems. the WWW is an emerging technology area that DOD can leverage to provide to the warfighter the information that is needed on the future battlefield in a timely and efficient manner. Analysis of the use of the WWW will occur in Chapter Four of this thesis.

---

[1]Alvin and Heidi Toffler, War and Anti-War: Survival at the Dawn of the 21st Century, (New York: Little Brown, 1993), 17 in Robert Walz, "Describing the Internal Security Environment: The Clash of Ideas"; excerpt reprinted in the US Army Command and General Staff College, C510 Syllabus/Book of Readings (Fort Leavenworth: USACGSC, 1 August 1995), 75.

[2]Lenny Zeltser, (1995), *The World-Wide Web: Origins and Beyond* [On-line]. Available WWW: http://homepage.seas.upenn.edu/~lzeltser/www/.

[3]Department of the Army, Army Enterprise Strategy: The Vision (Washington, DC: Government Printing Office, 20 July 1995), 32.

[4] George Morzinski, "Global Grid Overview" RESHAPING C3I 1993 AFCEA SYMPOSIUM, FORT MONMOUTH CHAPTER (Eatontown, NJ: AFCEA, September 1993), I-4.

[5]The Joint Staff, "C41 FOR THE WARRIOR GLOBAL COMMAND AND CONTROL SYSTEM: FROM CONCEPT TO REALITY," (Washington, DC: U.S. government Printing Office, 12 June, 1994), 10.

[6]Zeltser, *The World-Wide Web* [On-line].

[7]Ed Kroll, (1993), *FYI on "What is the Internet"* [On-line]. Available gopher:// ds.internic.net.00 /fyi/fyi.20.txt

[8]Kroll.

[9]Kroll.

[10]Kroll.

[11]Zeltser *The World-Wide-Web* [On-line].

[12]P. Hotzel, P. LaCount, S. Popham, and J. Rutter, Integrated Tactical Strategic Data Networking -Army (ITSDN-Army) Program Plan (Draft) (Washington, DC: MITRE Corp, May 1995), 1-2.

[13]P. Hotzel, P. LaCount, S. Popham, and J. Rutter, 2-6.

[14]U.S. Defense Information Systems Agency, Integrated Tactical-Strategic Data Networking "Quick-Fix" Engineering Plan, Intra-Agency Coordination Draft (Washington, DC: U.S. Government Printing Office, 12 May 1995), 5-6.

[15]DISA, ITSDN Engineering Plan, 5.

[16]DISA, ITSDN Engineering Plan, 5-6.

[17]DISA, ITSDN Engineering Plan, 6.

[18]DISA, ITSDN Engineering Plan,., 9.

[19]DISA, ITSDN Engineering Plan, 1.

[20]DISA, ITSDN Engineering Plan, 3-4.

[21]DISA, ITSDN Engineering Plan, 2.

[22]U.S. Defense Information Systems Agency, Joint Interoperability and Engineering Organization, Joint Task Force Tactical Communications Architecture Overview, JIEO Report 8125 Overview (Washington, DC: U.S. Government Printing Office, March 1995), 2-9.

[23]DISA, Architecture Overview, 2-9.

[24]DISA, Architecture Overview, 2-9.

[25]MG Campbell, ABCS Implementation Briefing for MG Joe Rigby 30 June 1995 (Ft Monmouth, NJ: Program Executive Office Command and Control Systems, 30 June 1995).

[26]DISA, Architecture Overview, 2-9.

[27]DISA, Architecture Overview, 2-10.

[28]DISA, Architecture Overview, 2-9 - 2-10.

[29]Clarence A. Robinson, Jr., "*Defense Organization Safeguards War Fighter's Information Flow*", SIGNAL, (Fairfax, VA: FEB 1996), 35.

[30]The Joint Staff, "C41 FOR THE WARRIOR GLOBAL COMMAND AND CONTROL SYSTEM: FROM CONCEPT TO REALITY", 12 June 1994, excerpt reprinted in U.S. Army Command and General Staff College C510 DJCO Command and Control reference Text Supplement, (Fort Leavenworth: USACGSC, June 1995), 4.

[31]Joint Staff.

CHAPTER 2

LITERATURE REVIEW

Summary

The C4IFTW program has received much recent attention. Many periodicals and military journals have provided an in-depth study of the C4IFTW program. These journals include titles such as Jane's Defense Weekly, SIGNAL, Military Intelligence, Marine Corps Gazette, Armed Forces Journal International, Military Technology, National Guard, Defense Electronics, JFQ: Joint Forces Quarterly, Journal of Electronic Defense, US Naval Institute Proceedings. Special Warfare, Asian Defense Weekly, Journal of Soviet Military Study, Government Executive, and Army.

Technical reports and engineering plans developed by both civilian and military organizations provided information on the C4IFTW program. Organizations, such as DISA, are frequently developing reports and plans that address the implementation of various components of the C4IFTW program. These reports address the use of WWW technology within the C4IFTW program. The JWID 1995 Demonstration Report was examined to review the use of WWW technology within the C4IFTW program.

The WWW is a source with information on the areas of research that are to be addressed within this thesis. One element of the C4IFTW program that has potential to use WWW technology is the Global Command and Control System (GCCS). DISA maintains a home page concerning the GCCS program on the WWW. This home page provides information on the GCCS program to include the meeting schedules, previous minutes, briefings, and procedures developed for the program. The GCCS training plan, mission needs statement, user interface specifications,

and integration standards are also available through this home page. Additional points of contact are provided with listings of the engineering department staff, architecture oversight group, and both the technical and style working groups. The GCCS software repository system is also accessible through this home page.

The DISA GCCS home page is linked to other DISA home pages, the Naval Postgraduate School home page, and DefenseLINK. These home pages provide additional information on research areas as well as additional links to other home pages. DefenseLINK is the home page maintained by the Department of Defense. DefenseLINK is a starting point for locating information relating to the Department of Defense located on WWW servers throughout the world. DefenseLINK provides access to information services established by the military departments and organizations as well as containing defense publications, frequently asked questions(FAQs), and an interface to the Government Information Locator Service (GILS). GILS information can be browsed and searched.[1] DefenseLINK provides multiple sources of information on both the C4IFTW program and GCCS.

The Internet and the WWW also provided information on the technology required to implement the WWW on the battlefield. Numerous home pages contain information on equipment and procedures necessary for the establishment of WWW type services. Information exists in hard copy form and also in electronic form on the Internet. Reports on the Internet and WWW have been published by NASA, the Defense Technical Research Center, the Department of Defense(DOD), and Carnegie-Mellon University. New articles and reports continue to be published in print and on the WWW that address both the WWW and the Internet.

There has been little information published on the incorporation of WWW technology into the C4IFTW program. Much of the C4IFTW program has applications, such as the ability to communicate with other computers and networks both horizontally and vertically, that are similar to those on the Internet. Techniques developed for the Internet should be applicable to parts of the C4IFTW program.

Journals

Jane's Defense Weekly is a source of Information on military technology available throughout the world and provides information on both US and allied equipment having an impact on the C4IFTW program. Although the C4IFTW program is primarily a US program, it will traverse and interface with foreign military communications on combined operations. Foreign military equipment of select countries was not examined in this thesis to determine their requirements for interface to U. S. equipment and networks to include the GCCS systems. Members of NATO and nations in the Middle East in particular are countries requiring examination. Other publications that provide similar information include: Armed Forces Journal International, Asian Defense Weekly, and the Journal of Soviet Military Study.

The Armed Forces Communications-Electronics Association (AFCEA) publishes SIGNAL magazine. AFCEA is a military defense industry organization that keeps the military and industry aware of new developments occurring in both military and civilian communications programs with potential military applications. SIGNAL is published monthly by AFCEA and usually adopts a specific theme each month. C4IFTW and GCCS have been monthly themes in the past for SIGNAL. AFCEA also publishes and distributes books on topics concerning military-related communications technology in addition to conducting frequent seminars that address the application of this technology.

Many branches of the military publish monthly periodicals related to their branch. These publications address new developments in both doctrine and technology within their respective branches. Many of the journals address recent developments concerning C4IFTW, FORCE XXI and the application of these new developments to the doctrine and techniques of the branch. These publications include Armor, Infantry, Special Warfare, and the Army Communicator. The Army Communicator is published by the US Army Signal Center(SIGCEN). SIGCEN is heavily

involved in FORCE XXI information management, DMS, and C4IFTW and publishes articles addressing these issues on a regular basis.

Other services within the Department of Defense also publish journals addressing their specific arm of the service. These journals include Army, Marine Corps Gazette, and the US Naval Institute Proceedings. The C4IFTW program deals with all of these aspects of communications. The military services are developing new procedures to improve internal and external communications. Many of these improvements are a direct result of the C4IFTW program and deal with aspects such as increased bandwidth and ease of use of communications systems. The journals published by each of the services continue to address the implementation of the C4IFTW program in the various military services.

The National Research Council(NRC) recently published a study titled "Commercial Multimedia Technologies for Twenty-first Century Army Battlefields, A Technology Management Strategy." This study was prepared by the NRC as a result of a request from the Army to study the application of commercial multimedia technology to Army communications systems. This study provides the Army leadership with findings that can assist the Army in its transition into the twenty-first century and demonstrates that current emerging commercial multimedia technology can greatly influence the future Army, but the Army must devise methods to accommodate the rapid change occurring in the commercial communications arena.[2] The WWW is one small portion of the current emerging commercial communications arena. The WWW will be examined in this thesis for applicability to the C4IFTW program.

Theses

Numerous theses have been published on the C4IFTW program. These theses have been published at the Massachusetts Institute of Technology, the Army Command and General Staff College, the Naval War College, the Naval Postgraduate School, the Air War College, and the Industrial College of the Armed Forces. Another source of published material includes the US Marine Corps Communications Officer School. The documents from military sources provided

good background information on the C4IFTW program in addition to providing good sources of additional research material in their bibliographies. These documents were available in both hard copy and microfiche at the US Army Combined Arms Research Library at FT Leavenworth, KS.

DOD Documentation

Documents published by DISA provide information on the C4IFTW program. DISA is responsible for the engineering and implementation of the strategic portion of the C4IFTW program. DISA is also responsible for the design, installation, operation, and maintenance of the tactical to strategic communications gateways. Numerous engineering plans have been published that address these issues. These documents were referenced in this thesis.

DISA is the lead organization on the ITSDN program. The ITSDN program is the military Internet that spans both the battlefield and the strategic networks. The ITSDN Program Plan was published by DISA on 22 June 1992. This document established the initial program concept, architecture, activities, and responsibilities. The initial milestones and schedules were also published in this document.[3] This document is useful for identifying the original need for the ITSDN program. Capabilities that are necessary on the battlefield are addressed in this document.

The ITSDN Quick Fix Concept of Operations was published by the DISA Data Services Development Division on 17 December 1993. This document addresses the necessary relationships for internetworking between tactical and strategic data networks.[4] WWW technology has the capability to be implemented across these networks.

The ITSDN DCS GMF Entry Point Implementation Plan was published by DISA on 6 July 1994. This plan establishes the implementation for tactical to strategic data communications at Defense Communications Systems(DCS) Ground Mobile Forces (GMF) Entry Points.[5] This program is critical for users on the battlefield to have tactical to strategic WWW access as well as allowing strategic users to access WWW servers on the tactical battlefield.

DISA published the proposed "DISN Near-term Security Architecture" on 21 May 1992. This document formulates a near term security architecture for the DOD data networks. This

security architecture addresses user connectivity and security requirements at the present capability level.[6] Any WWW services implemented on DOD data networks would have to meet these security requirements.

Each of the services has various organizations responsible for both the procurement of communications equipment and the development of communications doctrine. These organizations include the US Army Communications Electronics Command(CECOM), SIGCEN, the US Air Force Air Combat Command(ACC), the US Air Force Electronic Systems Command(ESC), the US Navy Space Warfare Command(SPAWAR), and the US Marine Corps Systems Command(MARCORSYSCOM). All of these organizations are involved in research and the development of doctrine and new equipment for the C4IFTW program.

A source of information for this thesis are test reports that are published on the annual Joint Warfighter Interoperability Demonstrations(JWID). JWIDs have been occurring annually since the late 1980s as a series of exercises that focus on providing the Joint community with innovative advances in Command, Control, Communications, Computers, and Intelligence(C4I) systems. The JWID exercises provide an operational overlay of C4I systems across Joint and Combined forces. The seventh JWID occurred in 1995. The purpose of JWID is to demonstrate improved capabilities for deployed warfighters and improved interoperability between existing and newly developed C4I systems. The Marine Corps was designated by the Joint Staff as the lead agency for JWID 1995 and the US Pacific Command (PACOM) was designated as the hosting Commander in Chief.[7] JWIDs are opportunities for defense contractors to demonstrate new capabilities in communications equipment. Much of the equipment that is successfully demonstrated during JWID will be a part of the future C4IFTW program. The services also use the JWIDs to demonstrate and test new concepts in doctrine. the WWW were demonstrated during JWID 1995. By examining the JWID test reports, a determination can be made as to what new developments in WWW technology have potential to be implemented in the C4IFTW program. Unsuccessful JWID contractor demonstrations point out what technologies will not work within the

C4IFTW architecture and provide insight to both contractors and the services on where to concentrate their efforts. The Army Battle Labs, which also serve as contractor testbeds and as a place for the Army to test new developments in doctrine on a year round basis, were involved in JWID 1995.

Industry Trade Journals

There are numerous trade journals published by the computer industry that address numerous aspects of emerging commercial multimedia technology from both a system and network perspective. Two of these publications used as research resources for this thesis are INFOWORLD and NETWORK WORLD. INFOWORLD is known as the voice of personal computing in the enterprise; it addresses new developments from a systems aspect. NETWORK WORLD is known as the news weekly of enterprise network computing; it addresses new developments from a network aspect.

Internet

The Internet is also a source of information concerning the WWW, the C4IFTW program, and the GCCS program. Numerous existing WWW pages are directly related to the C4IFTW and GCCS programs and provide information on the WWW and the Internet. Programs that have WWW pages are the GCCS program, the DMS program and the FORCE XXI program. Several WWW pages address techniques on how to prepare documents in Hypertext Markup Language (HTML), the language of the WWW. These WWW pages contain relevant information as well as provide connectivity to other WWW pages that contain additional relevant information.

Many of the organizations listed in the previous paragraphs also have WWW pages. Numerous organizations within DOD maintain WWW pages. The DISA GCCS home pages were accessed to collect information about the GCCS program. These homepages contained a variety of information to include the most current information on the recent developments to the GCCS program.

The WWW contains a wealth of information about itself. The document The World-Wide Web: Origins and Beyond by Lenny Zelster is available on the WWW. Many other references are cited in this article, and these documents can be referenced using the WWW.

---

[1]Department of Defense, (1995), *About DefenseLINK*, [On-line]. Available: WWW: http://www.dtic.dla.mil/ defenselink/about.html.

[2]Committee on Future Technologies for Army Multimedia Communications, National Research Council, Commercial Multimedia Technologies for Twenty-first Century Army Battlefields (Washington, DC: National Academy Press, 1995), v.

[3]U.S. Defense Information Systems Agency, "Integrated Tactical-Strategic Data Networking "Quick-Fix" Engineering Plan, Intra-Agency Coordination Draft" (Washington, DC: U.S. Government Printing Office, 12 May 1995), 4.

[4]DISA, ITSDN Engineering Plan.

[5]DISA, ITSDN Engineering Plan.

[6]DISA, ITSDN Engineering Plan.

[7]U.S. Defense Information Systems Agency, D8 C4I Modeling, Simulation & Assesment and the Joint Interoperability Test Command, Joint Warrior Interoperability Demonstration 1995, Demonstration Report (Washington, DC: U.S. Government Printing Office, Jan 1996), I1-I2.

CHAPTER 3

RESEARCH DESIGN

Research Approach

This chapter will address the methodology and criteria for analyzing the use of WWW technology within the C4IFTW program. The background information provided within this chapter will assist the reader in understanding a portion of WWW technology and how this technology may support the C4IFTW program.

The analysis for this thesis was based on a variety of sources. Magazines, journals, and trade publications provided information on this new and emerging technology. The C4IFTW program and the WWW are both immature efforts with new developments being reported frequently.

The analysis contained in Chapter 4 is information that was collected from the sources described above. The answer to the research question presented in Chapter 5 is a result of the analysis of this information.

Analytical Plan

The criteria used to conduct this thesis consisted of a review of various aspects of the C4IFTW program. The objective was to determine if WWW technology could provide timely and efficient exchange of information to support the warfighter. In order for the exchange of information to occur, the network connectivity must exist, WWW technology must be available for the warfighter, the necessary platforms to support WWW technology must be available, and the GCCS program must show the potential to use WWW technology.

This thesis began with a review of the C4IFTW program to include the existing tactical and strategic data networks. These networks were examined to determine if they are capable of supporting WWW services within the C4IFTW program. This analysis occurred in chapter four of this thesis. The capabilities of WWW technology must be studied to determine how its use would benefit the C4IFTW program.

A study of the equipment from the C4IFTW program determines how this equipment can support WWW technology within the C4IFTW program. Various components of equipment at different levels of command are most likely capable of addressing the various warfighter requirements. The Department of Defense is fielding new computer equipment for the GCCS program and various other command and control programs within.

The user requirements of the GCCS program are reviewed in this chapter. GCCS is a major component of the C4IFTW program and presents potential as a possible program that may be able to use WWW technology to meet its user requirements. Other components of the C4IFTW program may also demonstrate the potential to incorporate WWW technology but these elements will not be examined in detail in this thesis.

The use of WWW technology within the C4IFTW program will require that policy be established to address how WWW services are provided to the warfighter. The establishment of procedures, guidelines, editorial review, and security may be as a requirement if the C4IFTW program is to utilize WWW technology. Headquarters, Department of the Army (HQDA) has already established initial policy.

The results of JWID 1995 show the potential for the use of WWW technology to support the warfighter within the C4IFTW program. JWID 1995 was a demonstration of emerging technologies that could help the warfighter mission. WWW technology was one emerging technology demonstrated on JWID 1995.

WWW Technology

Examination of various elements of the WWW must occur in order to determine how this technology can support the C4IFTW program and how best to provide these services within the C4IFTW program. The user requirements mainly concern the exchange of information in a timely and efficient manner. WWW technology has the ability to provide a timely and efficient exchange of information.

An investigation of home pages, to include the format for data on the WWW and the Hypertext Markup Language (HTML), the home page scripting computer language, must occur so that a determination may be made on how to best implement this technology to support the C4IFTW program. The procedures for establishing and maintaining WWW browsers and servers, the computer programs that access and store the home pages, must also be investigated so that the necessary exchange of information can occur for the warfighter.

Home Pages

Home pages are the main documents on the WWW and are the first page that a user will see when accessing a site on the WWW.[1] A WWW site is a computer that a company, university, individual, government organization, or military unit maintains on the Internet or some internet-like communications network.[2] A home page can contain text, graphics, pictures, video and audio information, and hyperlinks. A home page may contain any text and graphical information that would be required by the warfighter on the battlefield. Hyperlinks will either be text (normally a different color than normal text) or a graphic, such as an icon. Hyperlinks give an individual the ability to open other documents on the WWW, on the current computer or on some other computer located on the network.[3] Hyperlinks enable people on the WWW to easily navigate the Internet and will allow the warfighter to link to various computers in the tactical and strategic network to get necessary and relevant information.

Each home page on the WWW has a unique address, known as a Uniform Resource Locator (URL, pronounced "earl"). A user, by knowing a URL, can navigate to a specific home page. An example format for a URL is http://www-cgsc.army.mil/cgsc/schedules.html:

1. http://--Describes the type of server the URL will open, where http represents a WWW server.

2. www-cgsc.army.mil--Describes the internet address for the WWW site where the home page is located.

3. /cgsc--The directory where the WWW home page is located

4. /schedules--This is the exact filename of WWW home page (NOTE: this filename can be longer than the eight characters allowed in DOS and Windows on other than DOS or Windows based servers.)

5. .html--An extension that describes the file type (Most WWW documents are written in hypertext markup language (html).) Note: The extension .htm may also be used.

URLs must be entered into a computer exactly as they are written in order to allow a user to reach a specific WWW page on the Internet.[4] Each element within the C4IFTW program that maintains a home page will have a unique URL. This URL is provided to the warfighters who need the information that will be maintained on each individual home page. If a warfighter does not have the necessary URL, he can still reach the home page by hyperlinks or by using a search engine to search the network to find the necessary information. Commercial search engines exist, providing the ability to search for information on the Internet.

Hypertext Markup Language (HTML)

WWW home pages are written using HTML. HTML is a language for placing presentation information in home page documents. This information, known as tags, describes how the documents are presented or viewed and how the documents are hyperlinked to other documents. HTML gives a WWW home page developer the ability to create interactive, cross-platform, multimedia, and client-server applications on the Internet.[5] Writing WWW home pages in HTML

allows users on the WWW access to information located throughout the Internet and will allow the warfighter access to information on the data network within the C4IFTW program.

Documents written in HTML are not computer programs and HTML is not a programming language. HTML specifies the grammar and syntax of the markup tags in the data that tell a browser (browsers described in later sections) how to present the data on a computer terminal.[6] HTML allows the underlying document to be presented with its associated text, graphics, pictures, video and sound, and associated hyperlinks.

HTML is not too complicated to prevent it from being used within the C4IFTW program. Warfighters, by learning a few simple rules and procedures, will be capable of developing HTML documents for posting on the network.

WWW Browsers

WWW browsers are the computer programs that enable an individual access to WWW information on the Internet.[7] Documents developed using HTML require HTML browsers for viewing on a computer terminal.

There are two types of WWW browsers, linemode and graphical. Linemode browsers run on a distant computer where they are connected as a remote terminal and use TELNET or a Bulletin Board System (BBS) for a connection. A linemode browser only allows the viewer access to text, not graphics or any multimedia information. A warfighter would be capable of getting text information on the network by using a linemode browser.

Graphical browsers are software programs that run on the actual machine that the viewer is currently working on and allow an individual to use the full capabilities of that machine's operating system.[8] Graphical browsers would allow the warfighter to utilize the full capacities of HTML and the WWW. Example graphical browsers are Netscape and Mosaic. Netscape is a commercially developed package. Mosaic was developed by the National Center for Supercomputing Activities (NCSA) at the University of Illinois-Urbana using US government funding and is available for free on the Internet. In order to run a graphical browser, the computer

that is running the browser must be on the actual Internet. The computer must be running some type of TCP/IP Internet networking software and connected to an actual Internet gateway. If the computer is not connected to the Internet, communications software running a Serial Line Interface Protocol (SLIP) driver or point-to-point protocol(PPP) driver is required to establish a phone connection to an Internet gateway.[9] Direct and dial-in gateways are currently available on various parts of the C4IFTW program to include both the Army TPN and the Air Force TASDAC at the tactical level and NIPRNET, SIPRNET, and JWICS at the strategic level. Warfighters have a variety of options for connecting to the data network to take advantage of WWW technology.

Commercial software companies are currently bundling WWW browsers and HTML authoring tools in commercially available software packages that run on desktop computers. Microsoft Corporation recently announced that HTML authoring and other collaborative computing features, to include indexing, viewing, and navigational tools, would be available in the Office[tm] suite of software.[10] Some of these tools may be currently downloaded for free from the Microsoft WWW home page (http:\\www.microsoft.com) Other software developers may follow Microsoft's lead and provide these type tools within their software. By using these tools the warfighter would not even have to learn HTML in order to prepare documents for posting on network.

SUN Microsystems Corporation's Java Language

The SUN Corporation's Java is a recent development impacting the WWW and the Internet. SUN describes Java in these terms:

> Java(tm) is a simple, object-oriented, distributed, interpreted, robust, secure, architecture-neutral, portable, high-performance, multithreaded, dynamic, buzzword-compliant, general-purpose programming language. Java supports programming for the Internet in the form of platform-independent Java applets.[11]

Java was developed to solve a number of problems with modern computer programming languages. Its origins can be traced back to the development of a computer language to develop advanced software for consumer electronics.[12] Java is intended to develop secure programs that work in

networked and distributed environments. Programs developed using Java are intended to be virus and tamper free.[13]

Java was developed to support computer applications that run on networks composed of computers using a variety of Central Processing Units (CPUs) and operating systems. Current software development requires that developers write a different version of software for each different type of computer platform, such as a PC or an Apple Macintosh. This is not required with Java since the same application can run on all platforms.[14] The use of compiled Java programs, known as applets, will make WWW browsers smarter by allowing WWW applications to run on the actual client instead of using bandwidth to maintain a connection with a WWW server located somewhere else in the network. Java applets could function as smart forms that allowed a user to input data and if the data was inputted incorrectly, the applet running on the client computer would catch the error before bandwidth was used to transmit the input data back to the server. Java applets can be developed to show animation of graphics and text, general and special purpose applications, and sophisticated user interfaces for smart push-warrior pull applications.[15] Java has the potential to reduce the amount of memory and processing power that the warfighter would require to exchange information.[16] The potential exists for Java to provide increased capability to the warfighter at little cost.

Many companies in the computer industry (Microsoft, IBM, Apple, DEC, Adobe, Silicon Graphics, Hewlett Packard, Oracle, and Toshiba) have recently come out in support of Java.[17] This industry support will most likely make Java a major factor on the Internet of the future. Many of these vendors hope that Java will shape the first generation of Internet-based client-server applications. Java is viewed as a compelling but not yet liberating technology.[18] Although Java is too new of a development to impact the current status of the C4IFTW program, it should be tracked for its future impact on all networks.

New developments continue to occur involving Java and a collaboration of vendors in the computer industry. Netscape Corporation, a major developer of WWW browser and server

software, is collaborating with SUN to develop a new language called Javascript which will allow developers to create WWW pages with audible and interactive screen elements.[19] The development of interactive WWW pages would greatly enhance the capability to develop user profiles for the smart push-warrior pull capability that is a goal of the C4IFTW program.

WWW Servers

Almost any type of computer with an interface to an Internet type network can function as a WWW server to include a diversity of systems such as Windows-based PCs, Apple Macintoshs, and UNIX workstations. All that is necessary for a computer to function as a WWW server is special server application software. The server software insures that the home pages maintained on the server present a consistent view to the network through the use of the HTML scripting language.[20] Many types of computers currently available on the battlefield are capable of functioning as a WWW server, meaning there is no requirement for a special type of computer to serve in this function. The military would not be required to spend money to buy high cost hardware to fulfill this requirement since many of the computers currently being fielded could meet the requirements to be a WWW server. IBM-compatible personal computers (PCs) running Windows software are capable of providing industrial strength WWW service at low PC prices.[21] There are numerous servers available. Some are available for free and can be downloaded from the WWW, and others can be purchased from vendors. The servers that are available from vendors usually provide better support.

WWW servers have the capability to execute special computer programs that allow them to serve as a gateway to information resources on the local system or on the network that the server is connected to include the Internet or some Internet type network. These types of programs are already available on the Internet and can be installed without modification or customized for a specific WWW site.[22] Commercial vendors are currently developing WWW servers with the capability to provide HTML authoring tools, data import/export converters and relational database management systems, all capabilities that may be of interest to the warfighter. Many vendors are

also announcing support for the Java language within their servers.[23] The capability that exists for WWW servers to serve as information gateways would enable the warfighter to have access to a variety of information that is available on the network.

Bandwidth Efficiency

WWW technology may be too bandwidth intensive and could overload the tactical networks. If the necessary bandwidth is not available, alternatives may be available for the warfighter to utilize WWW technology within the C4IFTW program. One alternative is the "gatekeeper" concept that could be used to support the warfighter deployed at a level where necessary bandwidth is not available but where e-mail is available. Gatekeeper personnel could be deployed at a level in the network where sufficient bandwidth is available for WWW services. A deployed warfighter could forward a request for information via e-mail to a gatekeeper who could conduct the necessary WWW search and return the information to the deployed warfighter through e-mail.[24] The gatekeeper concept enables the warfighter to use WWW services anywhere that e-mail services are available.

A second alternative would be the use of a product developed by MILKTRUCK LLC known as Milktruck Delivery which is a utility for WWW browsers. Milktruck Delivery allows users to capture WWW home pages and store them locally for viewing. Once a WWW home page is stored regular text updates could be scheduled to maintain currency of information. Test versions of Milktruck Delivery software can be downloaded for free at URL: http://www.milktruck.com.[25] Another product that offers a similar capability is WWW Arranger 2.0 from CE Software. WWW Arranger offers the capability to download WWW home pages for future viewing when disconnected from the network and the additional capability to poll WWW servers for updates to URLs.[26] If the necessary bandwidth is not available to provide full time WWW services to the warfighter, then either of these two alternatives may provide a solution.

Emerging WWW Technologies With Possible C4IFTW Applications

Developments in the area of data warehousing have the potential to impact the Internet and WWW. Data warehouses attempt to pull data from legacy data systems by merging data from multiple sources, reformatting the data, and allowing users to easily browse this data. The Internet is projected to be the standard medium for individuals to retrieve data that is stored in the data warehouses. WWW browsers will be used by individuals for access of the necessary information. Future technologies will combine databases, the Internet, intelligent agents, server-side processing and client-side editing of client server systems.[27] Many of the current DOD databases that the warfighter may need access to are legacy systems that may be converted to data warehouses with Internet type of access. Commercial vendors continue to develop products that will allow WWW access of databases. Microsoft Corporation's SQL Server 6.5 has the necessary tools to allow the warfighter to navigate and publish data to the Internet. This server will provide the capability to automatically update WWW home pages based on a predetermined schedule or a change in the source data. If an outage occurred somewhere in the networks, a transaction coordinator within the server will roll back all the servers in the network to the original state.[28] This server would allow the warfighter responsible for database administration to run distributed applications--a capability that would be necessary within the C4IFTW program. A software product developed by Parc Place-Digitalk, Inc., called Visual Wave will allow developers to build WWW application programs that will provide the warfighter with the capability to engage in two-way interactions with databases located on the network.[29] These capabilities would provide the warfighter with the capability for accessing information stored in databases throughout the C4IFTW network as opposed to only accessing information maintained on home pages. Another product recently developed by First Floor Software, Inc. is the Smart Bookmarks 2.0 program for the WWW. Smart Bookmarks offers the capability to monitor WWW servers for changes would assist the

warfighter in keeping track of current information.[30] This capability will provide the warfighter with a warrior pull capability.

Netscape Communications Corporation is developing a specification that will allow for the management of WWW servers with existing network management platforms using the Hypertext Transport Protocol (HTTP) Management Information Base (MIB). The HTTP MIB will define WWW server-related data that the warfighter will be able to use to manage WWW servers deployed within the C4IFTW program. The types of information that will be provided by the HTTP MIB include the number and type of requests for a specific home page, response time, and traffic statistics. If a WWW server stopped answering requests, a procedure could use the HTTP MIB to alert the warfighter.[31] The use of HTTP MIB technology within a network management program would provide the warfighter with an automated method to manage WWW technology on both the tactical and strategic networks.

Netscape also announced its intention to make its WWW browser compatible with real time audio, video, and data conference applications. This technology will allow the warfighter to place phone calls over the data networks. This capability would be bandwidth intensive, but this technology might lead to further developments in bandwidth compression technology. It is projected that the future of WWW is to merge real-time audio and video conference capabilities with graphical capabilities.[32] The ultimate goal of the C4IFTW program is a single network that would provides seamless connectivity for all of the warfighter's information requirements.[33]

Intelink

DOD in conjunction with the Director of Central Intelligence has established an Internet type intelligence information service known as Intelink. Intelink is a set of commercial Internet tools like WWW browsers and servers running on classified networks to include SIPRNET and JWICS. Intelink is intended to improve the distribution of intelligence information. There are more than 60 WWW servers on currently on JWICS. The network on SIPRNET known as Intelink-S is developing at a slower rate than the Intelink on JWICS. The potential user base for Intelink-s is

larger since there are more users of SIPRNET.[34] Intelink is a capability that the warfighter will require access for intelligence information. A warfighter using a computer equipped with a WWW browser and a connection to SIPRNET is able to access the WWW pages of Intelink-S.

C4IFTW Equipment to Support WWW Technology

Computers currently fielded to the warfighter may have the capability to support the implementation of WWW technology on the battlefield. If these computers can be connected to the ITSDN network and have sufficient memory and CPU power, they can function as either a WWW client (browser) or server. Many of these computers were fielded to support the various Battlefield Functional Areas (BFAs) and have the capability to connect to the tactical data networks.

There are several new communications systems that the Army is fielding under the C4IFTW program to support the deployed warfighter. One of these systems is GCCS described in Chapter One. The Army component of GCCS is known as the Army GCCS (AGCCS). AGCCS will be deployed at three levels: strategic, operational, and tactical. AGCCS is the intended replacement for current stovepipe systems and will utilize a common infrastructure. Connectivity between AGCCS terminals will be on SIPRNET at the strategic level and the ITSDN network at the tactical level. Tactical nodes will be capable of supporting strategic, operational and tactical users. AGCCS will be fielded at both the EAC and ECB levels throughout the Army.[35] The AGCCS program will interconnect the warfighter to the Global Grid.

The computer systems that will support the AGCCS program will be purchased off the Common Hardware/Software II (CHS II) contract. The CHS II contract provides a variety of computer equipment to include ruggedized systems for field use. These systems will provide connectivity through LANs, and remote access including dial-up and serial connection. The AGCCS servers will be SPARC 20, 1000, or 2000 computers where the choice of computers will be based on the number of users and the amount of information that will be stored on the computer. These computers are fully capable of hosting a variety of WWW server software and functioning as a WWW server for the warfighter. The users work stations will be SPARC 5/20 computers.

These systems are fully capable of running browser software and providing the warfighter with the capability to access WWW servers located on the tactical and strategic networks. Both the client and server computers have an adequate CPU and sufficient memory to provide WWW type services for the warfighter.[36] Computers that are capable of supporting the warfighter's use of WWW technology on the military data networks are already available in the GCCS program. The other services have programs that are similar to AGCCS that are also most likely fielding similar computers on the battlefield.

The Army ABCS program is also purchasing computers under the ATCCS program to support the warfighter on the battlefield down to the lowest tactical level. ABCS computers, purchased from the CHS contract, will include computers that are capable of supporting WWW services. The CHS contract includes the Lightweight Computer Unit (LCU) based on a 486 CPU, the Portable Computer Unit (PCU) based on a HP 9000 series 300 computer, and the Transportable Computer Unit (TCU) which is based on HP Reduced Instruction Set Computing Architecture. The LCU, PCU, and TCU are all capable of being networked and functioning as WWW browsers and servers.[37] Through both the GCCS and ABCS program a variety of computers will be available at all levels of command. Wherever the warfighter is computers will be available to support WWW services within the C4IFTW program.

Many companies that produce telecommunications and networking products are embracing WWW technology within their products. Banyan Systems, Inc., recently announced products and services that will move Banyan from the network operating system environment into the Internet environment.[38] The Marine Corps uses Banyan products in their tactical local area networks. Other commercial vendors used by DOD in the communications arena will also incorporate Internet and the WWW into their products if they have not already done so.

GCCS User Requirements

The five warfighting Commanders in Chiefs (CINCs) identified the user requirements for the GCCS program. The core functions that the CINCs identified are crisis planning, force

deployment, force employment, force status, logistics, air operations, fire support, intelligence, personnel, position, and narrative information.[39] These areas all have the potential for the application of WWW technology. Information updates, maps, and other graphics could be transferred using WWW technology in support of crisis planning and intelligence. Deployment data could be transferred in support of force deployment. The Air Tasking Order could be made available on a WWW server in support of air operations. Deployed warfighters could interface with databases located in the sustaining base for all types of information. Information to support the other areas could all be made available through the use of WWW technology.

Documents are available on the WWW that describe the user interface for GCCS. This user interface is being built in accordance with the Common Operating Environment (COE). The GCCS COE is the software infrastructure that supports the applications that GCCS provides to the warfighter. The COE includes support applications, platform services, and reusable software components. The COE Software Development Environment Description is in the COE documentation available on the DISA GCCS home page.[40] WWW applications that GCCS will contain include Mosaic, Netscape, and Netsite to allow for the maintenance and access of on-line documentation over the C4IFTW network.[41]

Other documents describe the background, purpose, and other factors that led to the development of the GCCS program. GCCS is a set of application programs configured to meet the needs of the commanders in the field. Some applications are general in nature, while others address a specific need of individual users. The overall goal of the GCCS program is to present the users with an interface that has a common appearance and behavior.[42] The GCCS program is attempting to develop a system that will provide a link between users and the data that the user requires so that the user can easily access and manipulate the required data in an efficient manner with minimal error. The GCCS system will allow users access to a variety of complex applications from a single system. It is for this reason that standardization is important, for it will allow for increased productivity, simplified training, higher reliability, and greater efficiency.[43]

This standardization may already be available within the technology that is available on the WWW.

There are a variety of data modules used within the GCCS COE to support the warfighter. The purpose of the data modules is to provide the information necessary to address the information requirements identified by the CINCs. One such data module is the Air Tasking Order (ATO) Review Capability Module. This module depends on e-mail to provide updates to the deployed warfighter through the C4IFTW network. The deployed warfighter can only use a text editor to review these ATOs.[44] The push of the ATO from higher headquarters to lower headquarters is the only capability that exists at the present time.

A second data module that currently exists within the GCCS program is the Fuel Resource and Allocation System. This module queries the JOPES database and collects the necessary information to generate flat files for use by PC based systems. The only types of data base that this module can access at present are the JOPES databases.[45] Formatted information must be available in the JOPES database before being accessed by this module.

Both the Air Tasking Order Review Capability and the Fuel Resource and Allocation modules can only access text based information in the present GCCS system. These modules do not have the capability for accessing graphical information and the ability to hyperlink to other databases is not available within the current GCCS COE. The capability for access of information other than text and the ability to hyperlink may be needed by the warfighter. Additional information and an analysis of the capability of WWW technology to support these GCCS modules is contained in chapter four of this thesis.

Policy Establishment for WWW Technology

The United States Army Training and Doctrine Command (TRADOC) recently released a memorandum dated 26 January 1996, Subject: "TRADOC WWW Guidance," that addresses these issues. An AUTODIN message from HQDA, DTG: 051348Z FEB 96 was released to establish policy for WWW home pages. The message stated that a review was necessary of the procedures

established to protect the information available through home pages as well as the procedures that insured the availability, confidentiality, and integrity of Army information. The message went on to state that the publishing of information on WWW home pages constitutes the public release of information and must comply with established Army policies and that any individual wishing to release Army information must have the appropriate public release authority. HQDA established the policy that the administrator who maintains the server where the information is being maintained assumes responsibility for ensuring that the information is properly cleared and that the appropriate safeguards are in place to prevent unauthorized access.[46]

DOD already has established an limited indexing service for information maintained on the unclassified DOD data networks. This service, known as DefenseLINK, is the official WWW Information Service from DOD. DefenseLINK is the starting point for unclassified DOD WWW servers located throughout the world. The purpose of DefenseLINK is to provide a single starting point for DOD information.[47] There are numerous commercial Internet indexing services that allow users to perform keyword searches of WWW information. These indexing services use software programs that search through the network processing information and compiling results into a database.[48]

The Army is currently conducting a survey on the Army use of WWW technology to support the exchange of information. In the past 18 months, the number of Army WWW sites grew from 40 to over 337. The vast majority of these Army sites exist in the strategic arena at fixed installations. The Army is using these sites to leverage technology to reduce the cost of traditional methods of communication, provide more accessible information, and increase efficiencies in daily functions. The purpose of this survey is to show the senior leadership of the Army that WWW technology is changing the way the Army works and communicates while saving money and time.[49] The results of this survey can be applied to the tactical elements of the C4IFTW program as well to provide justification for the incorporation of WWW technology within the tactical C4IFTW program.

Joint Worldwide Interoperability Demonstration (JWID) 1995

JWID 1995 was conducted in the fall of 1995 with the US Marine Corps as the lead service and the US Pacific Command (PACOM) as the lead CINC. The objective of JWID 1995 was to view emerging technology and relate it to the operational challenges of the US military. JWID examined many emerging technologies in the area of military communications and electronics that will enhance the method that the warfighter uses to share, access, process and disseminate information. WWW technology used during JWID 1995 increased the ability of the warfighter to exchange and access information. The use of WWW technology provided connectivity between US and allied forces.[50] JWID 1995 was the first official use of WWW technology within the Joint tactical environment.

The Joint Staff invited allied nations who are members of the Combined Communications Electronics Board to participate in JWID 1995. Australia, Canada, and the United Kingdom participated in the exercise. The All Source Analysis System (ASAS), an intelligence processing system, used WWW technology. ASAS used a WWW server that provided filters and served as a source of intelligence information for Combined Operations.[51] The use of WWW technology within the ASAS system allowed for the sharing of intelligence information with US allies.

A Collaborative Contingency Targeting demonstration integrated the Rapid Application of Air Power with COTS products for the sharing of information. A targeting WWW server provided collaborative targeting information to the warfighter. This demonstration allowed for coordinated priority targeting and damage assessment. The results of this coordination were published on a WWW server.[52]

The intent of the Structured, Preplanned, Environment, Access and Reference demonstration was to reduce the complexity and overload potential of information for a commander. Tailored information access with WWW technology matched the commanders normal decision making process and information presentation environment.[53] This demonstration is an instance of tailoring information to develop a smart push capability for the commander by

providing the commander with the information that he requires to make decisions without information overload.

The weather demonstration of JWID 1995 used home pages on the Tactical Forecast System and the Integrated Meteorological System to make weather information accessible to the C4IFTW network by using browser software.[54] This system has the potential to provide weather information to any browser equipped warfighter on the common user network.

During JWID 1995 WWW technology supported the warfighter in simulated operations other than war. Simulated images of hurricane and earthquake damage were collected from the Internet and distributed to the warfighter.[55] This demonstration is significant because it showed the potential for the warfighter to use the non-military portion of the Internet to gather mission critical information.

The JWID 1995 Demonstration Report Conclusions state that WWW technology enhanced information exchange between Allies and within the Joint Task Force. The use of WWW servers and browsers allowed the warfighter to electronically exchange information between system that had been non-interoperable. WWW technology exchanged information on the Common Operations Picture, the enemy situation, intelligence, weather, and imagery.[56] JWID 1995 demonstrated that there is a potential use for WWW technology to support the warfighter within the C4IFTW program.

---

[1]Jim Minatel, Easy World Wide WWW Access with Netscape (Indianapolis, IN: Que Corp, 1995), 26.

[2]Minatel.

[3]Minatel.

[4]Minatel.

[5] Larry Aronson, HTML Manual of Style (Emeryville, CA: Ziff-Davis Press, 1994), 1.

[6]Aronson.

[7]Minatel, 10.

[8]Aronson, 6.

[9]Aronson, 7.

[10] INFOWORLD, "Internet Tools coming to Office" (San Mateo, CA: International Data Group, 11 DEC, 1995). 24.

[11] SUN Microsystems, Inc, *About JAVA,* (1995), [On-line]. Available WWW: http://www.sun.com/about.html.

[12]SUN, *About JAVA.*

[13]SUN, *About JAVA.*

[14]SUN, *About JAVA.*

[15]Mark Gibbs, "*WAKING UP TO java*" NETWORK WORLD (Framingham, MA: Network World, 19 FEB 1996), 25-27.

[16]Andrew C. Braunberg, "*Device Offers Potentially Radical Shift in Computer Evolution*" SIGNAL (Fairfax, VA: FEB 1996), p 53-55.

[17]Phillip Elmer-Dewitt, "Why Java is Hot" Time (New York, NY: Time, Inc., 22 JAN, 1996), 59.

[18]Nick Wingfield, "Smell of Java lures scores of vendors" INFOWORLD (San Mateo, CA: International Data Group, 11 DEC, 1995). 1,20.

[19]Peggy Watt, "*Java Tool from Netscape and Sun no average Joe*", NETWORK WORLD, (Framingham, MA: Network World, 30 OCT 1995), 1,20.

[20]Edwin Mier, "*Off to the Races*" NETWORK WORLD (Framingham, MA: Network World, 19 FEB 1996), 4-10.

[21]WWW Site™, WWW Site Analysis, [On-line] Available: http://solo.dc3.com/white/wsperf.html

[22]Bryan Buus, Russ Jones, Cricket Liu, Adrian Nye, & Jerry Peek, Managing Internet Information Services, (Sebastopol, CA: O'Reilly & Associates, Inc., 1994), 287.

[23]Edwin Mier, "*Off to the Races*" NETWORK WORLD (Framingham, MA: Network World, 19 FEB 1996), 4-10.

[24]Jim Cavanagh, "*Using gatekeepers to avoid Internet abuse*" NETWORK WORLD (Framingham, MA: Network World, 8 JAN 1996), 37.

[25]Nick Wingfield, "*Milktruck pulls WWW data off-line*" INFOWORLD (San Mateo, CA: International Data Group, 5 FEB 1996), p 45.

[26]Jessica Davis, "*Email World/Internet Expo to feature WWW solutions*" INFOWORLD (San Mateo, CA: International Data Group, 19 FEB 1996), p 6.

[27]Andrew C. Braunberg, "*Data Warehouses Migrate Toward World Wide WWW*" SIGNAL (Fairfax, VA: AFCEA, FEB 1996), 35.

[28]Terence Ng and Yun Wang, "*SQL Server 6.5 opens the door to the World Wide* WWW" INFOWORLD (San Mateo, CA: International Data Group, 5 FEB, 1996). 93.

[29]John Cox, "*New tools ties WWW to back end aps*" NETWORK WORLD (Framingham, MA: Network World, 4 DEC, 1995), 12.

[30]Jessica Davis, "*First Floor tools monitor WWW site changes*" INFOWORLD (San Mateo, CA: International Data Group, 19 FEB 1996), 51.

[31]Mark Leon, "*Netscape's new specification eases Web server management*"INFOWORLD (San Mateo, CA: International Data Group, 5 FEB, 1996). 6.

[32]Nick Wingfield, "*Netscape WWW tools to gain conferencing*" INFOWORLD (San Mateo, CA: International Data Group, 5 FEB, 1996). 8.

[33] The Joint Staff, "C41 FOR THE WARRIOR GLOBAL COMMAND AND CONTROL SYSTEM: FROM CONCEPT TO REALITY", 12 JUNE 1994, (Washington, DC: U.S. government Printing Office, 12 JUNE, 1994), 2.

[34]DISA, *DISA Subject Index Page-Intelink*, (1996), [on-line], Available WWW:http://www.disa.mil/disasubj.htm#ltr.I

[35]John C. Sherrard, AGCCS SDR/SSR SYSTEM ARCHITECTURE BRIEFING, (Lockheed Martin, 18 OCT 1995).

[36]Sherrard.

[37]DCD, Ft Gordon, *ATCCS Material Requirements*, (1996), [on-line], Available WWW:http://www.gordon.army.mil/atccs.htm

[38] Kevin Fogarty, "Banyan reaches beyond VINES, grabs for 'Net" NETWORK WORLD (Framingham, MA: Network World, 12 FEB 1996), 25.

[39]The Joint Staff, "C41 FOR THE WARRIOR GLOBAL COMMAND AND CONTROL SYSTEM: FROM CONCEPT TO REALITY", 12 JUNE 1994, (Washington, DC: U.S. government Printing Office, 12 JUNE, 1994), 8.

[40] Defense Information Systems Agency, "GCCS BASELINE COMMON OPERATING ENVIRONMENT", (1995), [On-line]. Available: WWW: http://164.117.208.50/COE/COE0.html#ExecSummary.

[41]Defense Information Systems Agency, "GCCS SYSTEM INTEGRATION SUPPORT", (1995), [On-line]. Available: WWW: http://164.117.208.50/cgi-bin/mfs/01/sissum/vff.wp?#mfs

[42]Defense Information Systems Agency, "GCCS STYLE GUIDE FOREWORD", (1995), [On-line]. Available: WWW: http://164.117.208.50/style/intro.html.

[43]DISA,"GCCS STYLE GUIDE FOREWORD".

[44]DISA, "GCCS SYSTEM INTEGRATION SUPPORT".

[45]DISA, "GCCS SYSTEM INTEGRATION SUPPORT".

[46]owner-53listserv, *DA WWW Guidance* (7 FEB 1996, 5:08 PM), Available WWW: http://www.usma.edu/hypermail.

[47]Department of Defense, *About DefenseLink,* (1996), [On-line]. Available WWW: http://www.dtic.mil/defenselink/about.html.

[48]Nick Wingfield, *"Indexing services proliferate on WWW"* INFOWORLD (San Mateo, CA: International Data Group, 8 JAN, 1996). 45.

[49]Department of the Army, *Army Webmaster Survey,* (1996), [On-line]. Available e-mail: webmaster@WWW.hqda.army.mil.

[50]U.S. Defense Information Systems Agency, D8 C4I Modeling, Simulation & Assessment and the Joint Interoperability Test Command, Joint Warrior Interoperability Demonstration 1995, Demonstration Report, (Washington, DC: U.S. Government Printing Office, Jan 1996), i.

[51]DISA, JWID 1995, I-7.

[52]DISA, JWID 1995, DCP5-6.

[53]DISA, JWID 1995, KB-3.

[54]DISA, JWID 1995, WP-5.

[55]DISA, JWID 1995, CN-8.

[56]DISA, JWID 1995, C-2.

CHAPTER 4

ANALYSIS

Introduction

Chapter 4 is an analysis of the research presented in the previous chapters of this thesis. This information was applied to the research question in order to determine how best to implement WWW technology within the C4IFTW program.

The five warfighting CINCs identified the user requirements in the GCCS program as being necessary for the warfighter. WWW technology and the tactical and strategic networks that exist in DOD are analyzed to determine if the capability exists within these elements to satisfy the identified user requirements. The existing data networks within the C4IFTW program are examined to determine if they can provide the necessary connectivity to enable the warfighter to use WWW technology at both the tactical and strategic level. WWW technology is examined to determine if it can address the user requirements addressed in the GCCS program. Available equipment within the C4IFTW program is analyzed to determine if it can support WWW services.

Network Architecture

In order for WWW technology to be available to support the warfighter, the necessary data networks must be in place to provide connectivity. These networks must be similar to or extensions of the Internet in order to utilize WWW technology. Both the tactical and strategic networks must be examined to determine if they are capable of supporting WWW technology.

The strategic networks developed and maintained by DISA were described in Chapter One. These networks were developed to support data communications on the posts, camps and stations belonging to DOD. The original unclassified network, MILNET, was an original component of the

Internet as developed by the ARPA. MILNET and its replacement NIPRNET, are still connected to the global Internet. A warfighter with a connection on NIPRNET and equipped with browser software is able to access WWW information located throughout the Internet. DSNET1 and its replacement, SIPRNET, are not connected to the Internet. These networks run at a higher classification level (secret) and are physically separate networks. These networks do have the same functionality as the Internet. A warfighter holding the proper security clearance (secret) with a connection on SIPRNET and browser software would be able to access information on a WWW server located on SIPRNET. The same hold true for DSNET3/JWICS. The data portion of JWICS is a network with Internet functionality that is already supporting the WWW.

Each of the services has developed a data network to meet their needs in the area of data communications. The individual data networks were described in detail in Chapter One of this thesis. Each of these data networks are capable of providing WWW services to their respective services.

The Army Tactical Packet Network (TPN) is a commercial standards based secret network that is similar to SIPRNET on the strategic network. The TPN is a network running the same TCP/IP protocols that run on the Internet and is capable of providing an Internet type network, to include WWW services, for the deployed Army. The TPN was fielded by the Army to support the various battlefield functional areas who would be able to use WWW technology to better support their programs by allowing for the warfighter easy exchange of information on the TPN.

The Army developed the Mobile Gateway Van (MGV) to provide for unclassified network traffic for the deployed Army warfighter. The MGV was described in detail in Chapter One and was developed to serve as a forward deployed MILNET/NIPRNET host for deployed Army units requiring connectivity to the unclassified DOD networks and the Internet

The Air Force developed the TASDAC to provide deployable and secure data communications with access to the strategic networks. TASDAC is also a commercial standards based network utilizing the TCP/IP protocol that runs on the Internet and supports the WWW.

The Marine Corps uses Banyan Vines to establish LAN networks when deployed. The Navy already has a tactical to strategic network established to connect its deployed elements (afloat) with the shore. The establishment of shore connectivity is through the Naval Computer and Telecommunications Area Master Stations to the unclassified networks (MILNET/DSNET1) and classified networks (DSNET1/SIPRNET) at the secret level and DSNET3/JWICS at the TS-SCI level).

The Joint Staff established the ITSDN program, addressed in Chapter One to improve tactical to strategic connectivity and tactical to tactical connectivity between the services in the area of data communications. The ITSDN program is intended to provide the warfighter with the ability to communicate with other services and the sustaining base and is a necessary component to allow the warfighter to be able to use WWW services to access information on the DOD Global Grid network. The ITSDN program has already established connectivity between the services and to the strategic networks.[1] The Joint Interoperability Test Center (JITC) continues to conduct ITSDN tests involving new developments and new equipment.

WWW Technology

Home pages are capable of serving as information repositories to support the warfighter by containing text, graphics, pictures, video and sound. The present data retrieval systems are primarily text based. The use of home pages will also allow the warfighter to hyperlink throughout the network to retrieve necessary information.

HTML can be easily used by the warfighter to develop documents to be posted on WWW home pages. The rules of HTML are simple to learn and products exist to develop HTML documents within a standard word processor. By using one of these products, some of which are currently available for free off the Internet, the warfighter would not even have to learn the rules of HTML.

WWW browsers are currently available to run on a variety of computer platforms. Several of these browsers are also available for free on the Internet. A warfighter using a

computer equipped with a browser and the necessary network software would have the capability for dial-in or direct connection within the existing C4IFTW data networks. WWW server software is also available to run on a variety of computers within the C4IFTW program. These browsers and servers will allow the warfighter access to information stored throughout the network.

The Java programming language being developed by the SUN Corporation has potential to influence the use of WWW technology within the C4IFTW program. Java applets can conserve bandwidth within tactical networks, allow smart forms to be developed for user interfaces that can develop smart push-warrior pull applications. Other alternatives beside Java are currently available to conserve bandwidth on the tactical networks. These alternatives, to include the gatekeeper concept and products such as MILKTRUCK Delivery Web Arranger 2.0, or Smart Bookmarks, all described in Chapter Three, could be implemented within the C4IFTW program. These products also allow for smart push-warrior pull to be implemented by polling home pages for updates.

The developments that are occurring in the area of data warehousing have definite potential for application within the C4IFTW program. Many of the existing DOD databases are legacy systems that can only be accessed through specific applications. The use of data warehousing, combined with WWW technology, would allow the warfighter access to information stored on any DOD network within the C4IFTW program. Products such as Visual Wave, described in chapter three, allow for two way interaction with legacy databases using WWW technology

WWW technology was used extensively on the recent JWID 1995 exercise. New technologies, to include the WWW, were described in the JWID 1995 demonstration report as technologies that will change the way the warfighter will share, access, process, and disseminate information. The use of WWW technology on both tactical and strategic networks during JWID 1995 enhanced the capability of the warfighter. JWID 1995 showed that WWW technology can support various C4IFTW programs.

Products are also being developed to use WWW technology for management of WWW servers that are deployed on the C4IFTW network. The deployment of WWW technology within the C4IFTW program will have an impact on the warfighter. A recommendation from JWID 1995 was that an integrated concept of operations be developed for the use of WWW technology.[2] This concept of operations could address WWW management. The specifications being developed by Netscape, described in chapter three, will allow the warfighter to manage the WWW servers deployed throughout the C4IFTW network.

C4IFTW Equipment to Support WWW Technology

There is a variety of C4IFTW computer equipment capable of supporting the implementation of WWW technology on the battlefield. These computers have sufficient computational power and memory to function as either a WWW browser or server. Two examples of such programs are the AGCCS program and ABCS programs reviewed in chapter three. These programs will field computers that will be available at a variety of command levels.

The AGCCS program is fielding computers that are replacing current legacy stovepipe systems. Connectivity for AGCCS will be on SIPRNET at the strategic level and through the services Secret high tactical data networks at the tactical level. These networks are part of the ITSDN program.

The ABCS program is currently fielding computers down to the lowest tactical level on the battlefield. These computers are intended to provide automated support for a variety of Battlefield Functional Areas. The capability will exist on the battlefield to use WWW technology to support the various BFAs. The use of the WWW for these systems would result in greater capabilities and efficiencies by allowing the users on one computer system to access information on another computer system within the ITSDN network.

Both the AGCCS and ABCS programs are using computers that are being purchased from the CHS contract. This contract contains a variety of computers that are fully capable of

connecting to the C4IFTW network and providing WWW services as either a WWW browser or server.

WWW Technology to Support GCCS User Requirements

GCCS is a major component of the C4IFTW program and will be available to support the warfighter at both the tactical and strategic levels. The GCCS user requirements identified by the CINCS address the requirements necessary for most automated systems on the modern battlefield. These requirements address the processing and exchange of information. WWW technology has the potential to support the exchange of information in support of the warfighter.

GCCS is intended to develop a single system that will provide a method for the warfighter to be able to link to the necessary data on the battlefield. The COE of GCCS is a collection of modules that provide support applications, platform services, and reusable software components. The WWW browsers Mosaic and Netscape and the WWW servers Netsite are components of the COE within the GCCS System Integration Support Document, published by DISA. This document does not state the specific uses of these components within the GCCS program.

An examination of two of the GCCS modules addressed in Chapter Three show that there is potential for specific applications of WWW technology within the C4IFTW program. The first module is The ATO Review Capability Module. This module intends to use e-mail to provide ATO updates to the warfighter. An alternative may be to create the ATO using HTML and post it on a WWW server and allow the deployed warfighter to use a WWW browser to view and retrieve this information. A product such as Milktruck Delivery or Web Arranger 2.0, described in chapter three, could be used by the warfighter to provide scheduled or automatic updates of the ATO. The use of WWW technology would allow for the warfighter to perform warrior pull over the communications network for necessary information as opposed to having this information pushed down from higher headquarters.

The Fuel Resource and Allocation System has potential use for WWW technology to support the warfighter. The GCCS System Integration Support Document states that this system

will query the JOPES database for specific information. This database access places a burden on the warfighter to insure that all the necessary information for this module is maintained on the JOPES database. The use of WWW technology incorporated with data warehousing, described in Chapter Three, would allow the warfighter access to information stored in legacy databases. This capability allows the warfighter to use various databases throughout the network for gathering information. Products are available from several different manufacturers that incorporate data warehousing with WWW technology.

The ATO Review Capability module and Fuel Resource and Allocation modules are currently intended to access text based information. The use of WWW technology would allow the warfighter to access additional forms of information besides text to include graphics, photos, and map overlays.

Other modules within the GCCS COE that have the potential to use WWW technology include the Dynamic Analysis and Replanning tool, the Evacuation System, and the Global Transportation Network. Each of these modules has the requirement to access information located throughout the network. All of the GCCS modules that deal with the Joint Operations Planning and Execution System (JOPES) also have the potential to use WWW technology since these modules must access information from a variety of sources. The use of this technology would provide increased capabilities to the warfighter and allow for the implementation of smart push warrior pull.

The Dynamic Analysis and Replanning Tool (DART) is a module that will access Time Phased Force and Deployment Data (TFFDD) files. TFFDD data is used to prepare for a deployment by listing the previously determined order of units that will deploy into a theater for a specific mission. The DART module is intended to allow planners to retrieve, edit and analyze TFFDD data.[3] If the TFFDD data was accessible using the WWW, it could be easily updated, maintained, and accessed by the warfighter through the SIPRNET network.

The Evacuation System component of GCCS is a module that will be used by both the Joint Staff and the State Department. The intended use of this module is to identify potential evacuees located at embassies or consulates throughout the world. The Evacuation System is a message based module that collects the required information from a State Department formatted message. A database also exists for users to query for information to plan for an evacuation. If the necessary information for this module was available using WWW technology, information queries and updates could occur in a more timely manner.

The Global Transportation Module provides a transaction oriented, event driven, data transfer capability. The purpose of this module is to provide the CINCs with necessary transportation information.[4] If this information was available through the use of WWW technology, the CINCs would be easily able to view and manipulate this data.

The Joint Operations Planning and Execution System module is intended to provide client application software that will allow users to generate reports. Users will have the ability to create tables and other report types and the capability will also exist to access the JOPES core database.[5] These capabilities all currently exist on the WWW. If the JOPES module made use of WWW technology within the GCCS platform, the users would view a familiar and consistent interface.

The Need for Policy Establishment

DOD is already using WWW technology to provide for the exchange of information. Commands that use WWW technology must develop procedures and guidelines for the content of information maintained on WWW servers. A policy for editorial review must be established to ensure that the proper and necessary information is being maintained on the WWW servers. Guidance must be established concerning URLs, warning banners to inform users of the security classification of the information that they can access, size of files and graphics for efficient use of bandwidth, version of HTML that is used, and organization of information. Commands that utilize WWW technology should develop policies addressing the establishment and use of WWW technology within their commands in both strategic and tactical environments. If tactical data

networks are run at the classified level then there will not be an issue since the classified networks will not be connected to the Internet. If the tactical networks run at the unclassified level and connectivity is established with the Internet, policies must be established to address information release.

DOD established a limited search capability, called DefenseLINK, to provide an indexing service for the strategic unclassified DOD WWW home pages. There are several search engines available on the Internet. DOD must determine if a similar service should be established for the classified DOD networks. DOD may have to establish this type of service to support the warfighter within the C4IFTW program. Individual commands may also be required to establish this type of service for their specific portion of the tactical networks.

The results of the Army survey that is currently being conducted to evaluate the use of WWW technology to support the exchange of information can be used to provide information the senior leadership of the Army. The conclusions developed from this survey can be applied to the C4IFTW program.

JWID 1995

JWID 1995 used WWW technology in several demonstrations to provide a means for the warfighter to share, access, process, and disseminate information. WWW technology allowed for information exchange that had not been possible in the past. Use of WWW technology allowed for exchange of information with Allied nations and the collection of information on the non-military portion of the Internet. The JWID 1995 demonstration report did not identify any specific plan for the use of WWW technology within the C4IFTW program. The JWID 1995 report stated that WWW technology was used to enhance the warfighter's capability for information exchange and access. The report went on to state that WWW technology should continue to be developed by the C4IFTW community.[6] Future JWIDs should test expanded applications of WWW technology and incorporate new capabilities based on the WWW as they develop.

[1]Executive Agent-Tactical Switched Systems, *Quick Fix User's Manual*,(1995),[On-Line], Available WWW: http://eatss1.sed.monmouth.army.mil/introduction.htm

[2]Defense Information Systems Agency, D8 C4I Modeling, Simulation & Assessment and the Joint Interoperability Test Command, Joint Warrior Interoperability Demonstration 1995, Demonstration Report (Washington, DC: U.S. Government Printing Office, Jan 1996), C-5.

[3]Defense Information Systems Agency, "GCCS SYSTEM INTEGRATION SUPPORT", (1995), [On-line]. Available: WWW: http://164.117.208.50/cgi-bin/mfs/01/sissum/vff.wp?#mfs

[4]DISA, "GCCS SYSTEM INTEGRATION SUPPORT".

[5]DISA, "GCCS SYSTEM INTEGRATION SUPPORT".

[6]DISA, JWID 1995, C2.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

Chapter 4 has shown that the necessary elements exist to use WWW technology to support the warfighter within the C4IFTW program. WWW technology is currently available for the exchange of information to support the various requirements of the warfighter concerning information. The cost of implementing WWW services within the C4IFTW program are not extravagant; much of the necessary technology is currently available within the C4IFTW program or it is available freely on the Internet. The employment of WWW technology within the C4IFTW program is not so complex as to prevent the use of this technology by the warfighter. The strategic networks already exist to support WWW technology and are already being used to provide limited WWW services. Each service has a tactical data network that is capable of providing the necessary connectivity for WWW services and through programs such as ITSDN, the necessary tactical to tactical and tactical to strategic data connectivity is being established to support the warfighter. The necessary equipment exists within the C4IFTW program to provide the WWW for the deployed warfighter.

Software products exist to allow deployed warfighters to access legacy databases maintained on the strategic DOD data networks. This capability will allow the deployed warfighter access to a wealth of information.

One area that will have a major impact on the future of WWW and the Internet is the Java combined programming language and run-time environment being developed by the SUN Corporation. Java is being proclaimed as the next major iteration of WWW technology. Java will

allow for significant flexibility in working with divergent network structures and the need to integrate new technologies into an existing infrastructure such as the DOD data networks. Applets can be designed with specific functions and accessed in any sequence to provide flexibility in communications. Java has the potential to reduce the amount of memory and processing power required to exchange information.[1] The potential exists for Java to provide increased capability to the warfighter at little cost.

Recommendations

Modules within the GCCS program should be reviewed to determine if they have the potential to use WWW technology. Any application that will require more than one warfighter to access a GCCS server for information has the potential for the use of the WWW. The two applications of GCCS examined in Chapters Three and Four, the ATO Review Capability Module and the Fuel Allocation System, can both benefit from the use of WWW technology. These two modules require the warfighter to view information on a GCCS platform. Other modules addressed in Chapter Four also can benefit from the use of WWW technology. This information could be maintained on a WWW home page so that all warfighters could have a consistent view of this information. Any other module within GCCS that has the same requirements could use WWW technology.

DOD and the services must establish policy for the use of WWW technology, otherwise each subordinate command will develop its own methods and procedures for editorial review, information release, and security. TRADOC has already established such a policy that should be reviewed by both the Army and the Joint community. HQDA also released an official message in 1996 addressing policy for the use of WWW home pages by Army units. The other services may have already established their own WWW policies and these policies may differ from what has already been established. The Joint Staff should follow the Army lead and establish a joint policy for the implementation of WWW technology so that a corrective program, like the ITSDN

program that was addressed in previous chapters of this thesis, is not required for the joint use of WWW technology.

A search capability, similar to what is available on the Internet, must be established within C4IFTW to allow the warfighter to find the necessary information. The warfighter must have a consistent capability to find information within the C4IFTW program. The amount of information that could be available to the warfighter is enormous. The system that is developed for the warfighter must present a consistent and easy to use interface, otherwise the system will not be used. The warfighter must have the ability to quickly access the required information without being overloaded by excess information. A search capability would give the warfighter this capability.

Summary

There is tremendous potential for the use of WWW technology within the C4IFTW program to support the warfighter. The necessary equipment and networks are either already available or can be readily obtained by DOD. Elements of DOD and the Army are already using WWW technology at the strategic level, and could easily provide many of the same capabilities available at the strategic level to the tactical level. The use of a strategic technology by the warfighter in the tactical arena would greatly simplify deployment training requirements. Warfighters could use the same procedures to collect and process information, no matter where they are deployed.

New developments continue to occur involving the Internet and WWW that would ease the information burden on the warfighter and provide new capabilities. The areas of efficient use of bandwidth and the ability to access legacy databases are functions that would benefit the warfighter. The warfighter will always be able to use additional bandwidth to transmit and receive other forms of information besides text. This additional bandwidth will ultimately be used to provide for all types of communications, voice, data, and video, to be carried over the same network.

There is a wealth of information in legacy DOD databases that the warfighter may require to perform a mission. The personnel involved in the C4IFTW program must continue to track these developments to look for potential uses of new capabilities to support the warfighter.

---

[1]Andrew C. Braunberg, "Device Offers Potentially Radical Shift in Computer Evolution" SIGNAL (Fairfax, VA: FEB 1996), 53-55.

BIBLIOGRAPHY

Books

Aronson, Larry. HTML Manual of Style. Emeryville, CA: Ziff-Davis Press, 1994.

Buus, Bryan, Jones, Russ, Liu, Cricket, Nye, Adrian, & Peek, Jerry, Managing Internet Information Services. Sebastopol, CA: O'Reilly & Associates, Inc., 1994.

Committee on Future Technologies for Army Multimedia Communications, National Research Council. Commercial Multimedia Technologies for Twenty-first Century Army Battlefields. Washington, DC: National Academy Press, 1995.

Minatel, Jim. Easy World Wide Web Access with Netscape, Indianapolis, IN: Que Corp, 1995.

Morzinski, George. "Global Grid Overview" RESHAPING C3I 1993 AFCEA SYMPOSIUM, FORT MONMOUTH CHAPTER , Eatontown, NJ: AFCEA, September 1993, I-4..

Toffler, Alvin and Heidi Toffler. War and Anti-War:Survival at the Dawn of the 21st Century, (New York: Little Brown, 1993), p. 17 in Walz, Robert. "Describing the Internal Security Environment: The Clash of Ideas." Excerpt reprinted in the US Army Command and General Staff College, C510 Syllabus/Book of Readings. Fort Leavenworth: USACGSC, 1 August 1995.

Department of Defense Publications

Department of the Army. Army Enterprise Strategy: The Vision , Washington, DC: Government Printing Office, 20 July 1995.

Hotzel, P., LaCount, P., Popham, S., Rutter, J. Integrated Tactical Strategic Data Networking - Army (ITSDN-Army) Program Plan (Draft), Washington, DC: MITRE Corp, May 1995.

Sherrard, John C. AGCCS SDR/SSR SYSTEM ARCHITECTURE BRIEFING, (Lockheed Martin, 18 OCT 1995).

The Joint Staff. "C41 FOR THE WARRIOR GLOBAL COMMAND AND CONTROL SYSTEM: FROM CONCEPT TO REALITY." Washington, DC: U.S. Government Printing Office, 12 June, 1994.

U.S. Defense Information Systems Agency, D8 C4I Modeling, Simulation & Assessment and the Joint Interoperability Test Command, Joint Warrior Interoperability Demonstration 1995, Demonstration Report, Washington, DC: U.S. Government Printing Office, Jan 1996.

U.S. Defense Information Systems Agency, Joint Interoperability and Engineering Organization. Joint Tak Force Tactical Communications Architecture Overview, JIEO Report 8125 Overview. Washington, DC: U.S. Government Printing Office, March 1995.

U.S. Defense Information Systems Agency. Integrated Tactical-Strategic Data Networking Point of Presence Implementation Plan. Washington, DC: U.S. Government Printing Office, 24 October 1994.

U.S. Defense Information Systems Agency. Integrated Tactical-Strategic Data Networking "Quick-Fix" Engineering Plan, Intra-Agency Coordination Draft. Washington, DC: U.S. Government Printing Office, 12 May 1995.

Internet

DCD, Ft Gordon, (1996). ATCCS Material Requirements, [on-line], Available WWW:http://www.gordon.army.mil/atccs.htm

Department of Defense, (1995). About Defense Link , [On-line]. Available WWW:http://www.dtic.dla.mil/defenselink/about.html.

Defense Information Systems Agency, (1995). "GCCS BASELINE COMMON OPERATING ENVIRONMENT." [On-line]. Available WWW: http://164.117.208.50/COE/COE0.html#ExecSummary.

Defense Information Systems Agency, (1995). "GCCS SYSTEM INTEGRATION SUPPORT." [On-line]. Available WWW: http://164.117.208.50/cgi-bin/mfs/01/sissum/vff.wp?#mfs

owner-53listserv, (7 FEB 1996, 5:08 PM). DA WWW Guidance Available WWW: http://www.usma.edu/hypermail.

Department of the Army, (1996). Army Webmaster Survey, [On-line]. Available e-mail: webmaster@WWW.hqda.army.mil.

Defense Information Systems Agency, (1995)."GCCS STYLE GUIDE FOREWORD", [On-line]. Available: WWW: http://164.117.208.50/style/foreword.html.

Defense Information Systems Agency, (1995)."GCCS STYLE GUIDE INTRODUCTION", [On-line]. Available WWW: http://164.117.208.50/style/intro.html.

Defense Information Systems Agency, (1996), DISA Subject Index Page-Intelink, [on-line], Available WWW:http://www.disa.mil /disasubj.htm#ltr.I

Department of Defense, (1995), About DefenseLINK , [On-line]. Available: WWW: http://www.dtic.dla.mil/defenselink/about.html.

Executive Agent-Tactical Switched Systems, (1995). Quick Fix User's Manaul [On-Line]. Available WWW: http://eatss1.sed.monmouth.army.mil/introduction.htm

SUN Microsystems, Inc, (1995). About JAVA, [On-line]. Available WWW: http://www.sun.com/about.html.

WWW Site™, WWW Site Analysis, [On-line] Available: http://solo.dc3.com/white/wsperf.html

Zeltser, Lenny. (1995). The World-Wide-Web: Origins and Beyond, [On-line]. Available WWW: http://homepage.seas.upenn.edu /~lzeltser/www/.

Periodicals

Braunberg, Andrew C. "Data Warehouses Migrate Toward World Wide Web." SIGNAL, (FEB 1996): 35.

Braunberg, Andrew C. "Device Offers Potentially Radical Shift in Computer Evolution." SIGNAL, (FEB 1996): 53-55.

Cavanagh, Jim, "Using gatekeepers to avoid Internet abuse." NETWORK WORLD, (8 JAN 1996): 37.

Cox, John. "New tools ties WWW to back end aps." NETWORK WORLD, (4 DEC, 1995): 12.

Davis, Jessica. "Email World/Internet Expo to feature WWW solutions." INFOWORLD, (19 FEB 1996): 6.

Davis, Jessica. "First Floor tools monitor WWW site changes." INFOWORLD, (19 FEB 1996): 51.

Elmer-Dewitt, Phillip. "Why Java is Hot." Time, (22 JAN, 1996): 59.

Fogarty, Kevin. "Banyan reaches beyond VINES, grabs for 'Net'." NETWORK WORLD, (12 FEB 1996) 25.

Gibbs, Mark. "WAKING UP TO java." NETWORK WORLD,(19 FEB 1996): 25-27.

INFOWORLD, "Internet Tools coming to Office." INFOWORLD (11 DEC, 1995): 24.

Leon, Mark. "Netscape's new specification eases Web server management." INFOWORLD, (5 FEB, 1996): 6.

Mier, Edwin, "Off to the Races." NETWORK WORLD,(19 FEB 1996): 4-10.

Ng, Terence and Wang, Yun. "SQL Server 6.5 opens the door to the World Wide Web." INFOWORLD, (5 FEB, 1996): 93.

Watt, Peggy. "Java Tool from Netscape and Sun no average Joe." NETWORK WORLD, (30 OCT 1995): 1,20.

Wingfield, Nick. "Indexing services proliferate on WWW." INFOWORLD, (8 JAN, 1996): 45.

Wingfield, Nick, "Milktruck pulls WWW data off-line." INFOWORLD, (5 FEB 1996): 45.

Wingfield, Nick. "Netscape WWW tools to gain conferencing." INFOWORLD, (5 FEB, 1996): 8.

Wingfield, Nick. "Smell of Java lures scores of vendors." INFOWORLD, (11 DEC, 1995): 1,20.

Theses

Carter, John W. Information Management in a Joint Task Force. Monterey, CA: Naval Postgraduate School, 1993.

Fox, Robert D. Using Today's Technology to Improve Mobile C4I for the Operational Commander. Carlisle Barracks, PA: Army War College, 1993.

Garretson, Jerimiah. Controlling Challenges to Jointness: Initiatives for Command and Control. Newport, RI: Naval War College, 1993.

Kohlmann, James P. Winning the Information War: Challenges of providing Interoperable Information System Support to an Army-Led Joint Task Force. FT Leavenworth, KS: Command and General Staff College, 1994.

INITIAL DISTRIBUTION LIST

1. Combined Arms Research Library
   US Army Command and General Staff College
   1 Reynolds Ave.
   Fort Leavenworth, KS 66027-1352

2. Defense Technical Information Center
   Cameron Station
   Alexandria, VA 22314

3. COL Gary E. Bushover
   Director, Academic Operations
   USACGSC
   1 Reynolds Ave.
   Fort Leavenworth, KS 66027-1352

4. MAJ Randall L. Mackey
   Directorate of Information Management
   645 Biddle Blvd.
   Fort Leavenworth, KS 66027-2309

5. COL Kenneth R. Garren
   1009 Stonegate Drive
   Salem, VA 24153

6. Mr. John Caruso
   Executive Agent-Tactical Switched Systems
   Building 1210
   Fort Monmouth, NJ 07724

7. COL Robert Forrester
   Director of Combat Developments
   ATTN: ATZH-CD
   Fort Gordon, GA 30905-5000

8. COL Rolland Dessert
   Center for Army Tactics
   USACGSC
   1 Reynolds Ave.
   Fort Leavenworth, KS 66027-1352

9. LTC Emmett Perry
Center for Army Tactics
USACGSC
1 Reynolds Ave.
Fort Leavenworth, KS 66027-1352

CERTIFICATION FOR MMAS DISTRIBUTION STATEMENT

1. Certification Date: 17 /April/ 1996

2. Thesis Author: Major John Levine

3. Thesis Title: The Use of World Wide Web Technology Within the Command, Control, Communications Computers, and Intelligence Program.

4. Thesis Committee Members Signatures:

5. Distribution Statement: See distribution statements A-X on reverse, then circle appropriate distribution statement letter code below:

(A) B C D E F X SEE EXPLANATION OF CODES ON REVERSE

If your thesis does not fit into any of the above categories or is classified, you must coordinate with the classified section at CARL.

6. Justification: Justification is required for any distribution other than described in Distribution Statement A. All or part of a thesis may justify distribution limitation. See limitation justification statements 1-10 on reverse, then list, below, the statement(s) that applies (apply) to your thesis and corresponding chapters/sections and pages. Follow sample format shown below:

S A M P L E	Limitation Justification Statement	Chapter/Section	Page(s)	S A M P L E
	Direct Military Support (10)	Chapter 3	12	
	Critical Technology (3)	Sect. 4	31	
	Administrative Operational Use (7)	Chapter 2	13-32	

Fill in limitation justification for your thesis below:

Limitation Justification Statement	Chapter/Section	Page(s)

7. MMAS Thesis Author's Signature:

STATEMENT A: Approved for public release; distribution is unlimited. (Documents with this statement may be made available or sold to the general public and foreign nationals.)

STATEMENT B: Distribution authorized to U.S. Government agencies only (insert reason and date ON REVERSE OF THIS FORM). Currently used reasons for imposing this statement include the following:

1. Foreign Government Information. Protection of foreign information.

2. Proprietary Information. Protection of proprietary information not owned by the U.S. Government.

3. Critical Technology. Protection and control of critical technology including technical data with potential military application.

4. Test and Evaluation. Protection of test and evaluation of commercial production or military hardware.

5. Contractor Performance Evaluation. Protection of information involving contractor performance evaluation.

6. Premature Dissemination. Protection of information involving systems or hardware from premature dissemination.

7. Administrative/Operational Use. Protection of information restricted to official use or for administrative or operational purposes.

8. Software Documentation. Protection of software documentation--release only in accordance with the provisions of DoD Instruction 7930.2.

9. Specific Authority. Protection of information required by a specific authority.

10. Direct Military Support. To protect export-controlled technical data of such military significance that release for purposes other than direct support of DoD-approved activities may jeopardize a U.S. military advantage.

STATEMENT C: Distribution authorized to U.S. Government agencies and their contractors: (REASON AND DATE). Currently most used reasons are 1, 3, 7, 8, and 9 above.

STATEMENT D: Distribution authorized to DoD and U.S. DoD contractors only: (REASON AND DATE). Currently most used reasons are 1, 3, 7, 8, and 9 above.

STATEMENT E: Distribution authorized to DoD only; (REASON AND DATE). Currently most used reasons are 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10.

STATEMENT F: Further dissemination only as directed by (controlling DoD office and date), or higher DoD authority. Used when the DoD originator determines that information is subject to special dissemination limitation specified by paragraph 4-505, DoD 5200.1-R.

STATEMENT X: Distribution authorized to U.S. Government agencies and private individuals of enterprises eligible to obtain export-controlled technical data in accordance with DoD Directive 5230.25; (date). Controlling DoD office is (insert).